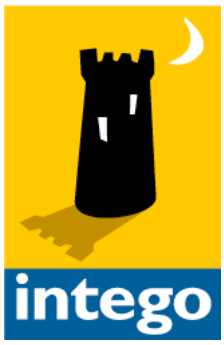
Manuel de l'utilisateur



Intego VirusBarrier X pour Macintosh

© 2000 - 2002 Intego. Tous droits réservés.

Intego 10, rue Say 75009 Paris, France
www.intego.com

Ce manuel accompagne le logiciel Intego VirusBarrier X pour Macintosh. Ce manuel et le logiciel Intego VirusBarrier X décrit ici sont protégés par copyright, avec tous droits réservés. Ils ne peuvent être copiés, sauf disposition contraire dans votre licence de logiciel ou par autorisation écrite expresse d'Intego.

Le logiciel appartient à Intego et à ses fournisseurs, et sa structure, son organisation et son code sont propriété d'Intego et de ses fournisseurs. Le logiciel est protégé par la loi sur les droits d'auteurs en France et les dispositions des traités internationaux.

Intego VirusBarrier X utilise les frameworks EDCommon et EDInternet écrits par Erik Dörnenburg.

Sommaire

1- A propos d'Intego VirusBarrierX *5*

Présentation d'Intego VirusBarrierX **6**

Fonctionnalités d'Intego VirusBarrierX **9**

Présentation du manuel d'utilisation **12**

2 - Introduction aux virus informatiques *13*

Raisons de se protéger **14**

Virus informatiques **14**

Auteurs des virus 16

Mode de fonctionnement des virus informatiques 17

Différents types de virus **20**

Virus système 20

Virus de fichiers 23

Canulars 26

Modes de propagation des virus 27

Modes de protection possibles contre les virus 28

3 - Installation *31*

Configuration matérielle et logicielle requise **32**

Installation d'Intego VirusBarrierX **32**

Enregistrement d'Intego VirusBarrierX **36**

Mode d'évaluation d'Intego VirusBarrierX **37**

4 - Prise en main rapide *38*

Mode par défaut d'Intego VirusBarrierX **39**

Interface d'Intego VirusBarrierX 40

Lancement d'une analyse manuelle **41**

Réglages de NetUpdate **44**

Analyse en glisser-déposer **46**

Utilisation d'Intego VirusBarrierX dans le Dock **46**

5 – Fonctions d'Intego VirusBarrierX ***48***

Analyse de virus **49**

Analyse manuelle 49

Analyse en glisser-déposer 57

Résultat d'analyse 57

Alertes **62**

6 – Réglages d'Intego VirusBarrierX ***63***

Préférences **64**

Options d'alertes 70

NetUpdate **72**

Encyclopédie de virus 73

A propos d'Intego VirusBarrierX **74**

7 - Diagnostic ***76***

Quelques symptômes d'infections **77**

Mesures de précaution élémentaires **79**

8 - Support technique ***80***

9 - Annexe ***82***

Glossaire **83**

Encyclopédie des virus **86**

1- A propos d'Intego VirusBarrier X

Présentation d'Intego VirusBarrier X

Intego VirusBarrier X est la solution de sécurité antivirus simple, rapide et non-intrusive à destination des utilisateurs d'ordinateurs Macintosh, proposée par Intego, l'éditeur du logiciel de sécurité personnelle, NetBarrier. Ce programme offre une protection efficace contre les virus de tous types, qu'il s'agisse de fichiers ou d'applications infectés résidant sur disquettes, CD-ROM, supports amovibles, ou de fichiers téléchargés sur Internet ou sur d'autres types de réseaux.

Intego VirusBarrier X protège votre ordinateur contre les virus en examinant constamment tous les fichiers lus et écrits par votre ordinateur. En installant Intego VirusBarrier X sur votre ordinateur, vous êtes assuré que votre Macintosh dispose de la meilleure protection possible contre les virus de tous types.

Intego VirusBarrier X est une application qui fonctionne en tâche de fond et inspecte toutes les opérations effectuées par votre ordinateur en vue de détecter des virus. Intego VirusBarrier X connaît les signatures uniques de tous les virus Macintosh connus. Par ailleurs, dès qu'un nouveau virus est découvert, l'équipe antivirus d'Intego s'active pour fournir des définitions de virus mises à jour, vérifiables automatiquement à l'aide de NetUpdate, la fonction unique d'Intego VirusBarrier X.

L'achat d'Intego VirusBarrier X vous donne accès aux définitions de virus mises à jour pendant un an à compter de la date d'achat. Après cette période, des abonnements additionnels, permettant de conserver l'accès aux définitions de virus mises à jour, sont disponibles auprès d'Intego ; vous pouvez souscrire sur le site Web d'Intego (www.intego.com) ou via NetUpdate.

Intego VirusBarrier X repose sur des concepts très spécifiques. L'idée clé étant qu'une fois installé et configuré, un programme antivirus ne doit pas nécessiter l'intervention de l'utilisateur tant qu'un virus n'a pas été détecté. La philosophie d'Intego VirusBarrier X peut se résumer en trois qualificatifs : simple, rapide et non-intrusif.

Simple

Intego VirusBarrier X est le programme antivirus pour Macintosh le plus simple et le plus facile à utiliser. Une fois installé, ce logiciel fonctionne en tâche de fond, veillant minutieusement sur votre ordinateur, et vérifie vos fichiers efficacement et en toute discrétion.

Rapide

Intego VirusBarrier X est rapide et efficace. Il ne ralentit pas votre ordinateur et vous n'avez pas besoin d'intervenir au cours de son exécution. À chaque écriture, utilisation ou ouverture de fichier, Intego VirusBarrier X effectue une vérification de manière à s'assurer que le fichier est sain.

Non-intrusive

Intego VirusBarrier X est non-intrusif. Ce logiciel ne vous assaille pas de questions suspicieuses chaque fois que vous installez un programme, pas plus qu'il ne vous importune en générant des « fausses alertes » incessantes. Une fois le logiciel installé, vous n'en remarquerez probablement pas la présence, à moins qu'il ne détecte un virus et ne génère une alerte. Par ailleurs, vous n'avez pas besoin de désactiver Intego VirusBarrier X lors de l'installation d'un nouveau logiciel, quoique vous préconise le programme d'installation ou le manuel de ce dernier.

Intego VirusBarrier X peut fonctionner en permanence, en tâche de fond, protégeant ainsi votre ordinateur sans nul besoin de s'en soucier.

Fonctionnalités d'Intego VirusBarrier X

Recherche de virus

Intego VirusBarrier X fonctionne de différentes manières. Il est constamment en veille, afin de protéger votre ordinateur contre les assauts éventuels de virus, et il peut également fonctionner en mode manuel. Vous pouvez ainsi lui demander d'analyser un disque ou un volume partagé de votre réseau. Intego VirusBarrier X recherche même les virus présents dans les archives Stuffit de fichiers compressés.

Réparations automatiques

Quand Intego VirusBarrier X fonctionne en mode automatique, il répare les fichiers infectés qu'il détecte en éliminant les virus ou vous indique qu'ils sont corrompus, selon les cas. Dans ce mode, vous n'avez nullement besoin de vous soucier de l'activité d'Intego VirusBarrier X – vous savez simplement qu'il est là, prêt à intervenir, dans le cas où un virus ou un fichier suspect serait détecté.

Analyse manuelle

Vous pouvez également utiliser Intego VirusBarrier X pour analyser manuellement vos fichiers. Il est recommandé d'effectuer cette opération dès l'installation du programme afin de vous assurer que votre ordinateur est sain. Vous pouvez par la suite utiliser cette fonction à tout moment et analyser manuellement des disques ou des volumes, vous assurant ainsi qu'ils sont exempts de virus.

Mode Turbo

Intego VirusBarrier X propose un Mode Turbo qui accélère les analyses. A la première analyse de votre ordinateur, Intego VirusBarrier X se souvient de tous les fichiers examinés. Tant que ces fichiers ne sont pas mis à jour, Intego VirusBarrier X ne les réanalyse pas, ce qui rend l'analyse de 5 à 40 fois plus rapide.

Rapport d'analyse

Intego VirusBarrier X affiche un rapport complet sur tous les virus ou fichiers douteux trouvés. Vous pouvez consulter ce rapport pour savoir si des fichiers ou applications sont infectés ou corrompus, les virus dont ils sont atteints et s'ils ont été réparés.

Dock

Si vous décidez de garder Intego VirusBarrier X dans le Dock, vous pouvez analyser les fichiers et les dossiers sans même ouvrir l'application ; il suffit de les faire glisser sur l'icône d'Intego VirusBarrier X.

NetUpdate

Intego VirusBarrier X dispose de NetUpdate, le programme d'Intego qui vérifie – automatiquement ou manuellement – l'existence de mises à jour du programme. Vous définissez la fréquence hebdomadaire de mise à jour et le programme interroge le serveur Intego, au jour et à l'heure indiqués. Si vous préférez procéder à des mises à jour manuelles, un simple clic de souris vous connecte au serveur et vérifie la présence éventuelle d'une nouvelle version.

Alertes de virus

Intego VirusBarrier X dispose d'options d'alerte pour que vous soyez averti en cas de détection d'un virus, lors de son utilisation en tâche de fond. Plusieurs types d'alerte sont disponibles : écran d'alerte, message vocal ou envoi de message électronique à une adresse déterminée. Cette solution peut s'avérer utile si vous souhaitez utiliser Intego VirusBarrier X sur des ordinateurs connectés à un réseau et avertir un administrateur réseau ou le propriétaire de l'ordinateur lorsque ceux-ci sont éloignés de leur ordinateur.

Présentation du manuel d'utilisation

Ce manuel d'utilisation offre des informations détaillées sur l'installation, l'utilisation et la mise à jour d'Intego VirusBarrier X. Vous y trouverez en outre une encyclopédie complète des virus Macintosh ainsi qu'un glossaire sur la terminologie des virus.

En premier lieu, nous vous invitons à lire l'introduction pour découvrir le mode de fonctionnement des virus (chapitre 2), puis à consulter la procédure d'installation (chapitre 3). Nous recommandons la description des fonctions d'Intego VirusBarrier X (chapitre 5) et des Préférences d'Intego VirusBarrier X (chapitre 6). Pour des informations détaillées sur les virus, consultez l'Encyclopédie des virus (chapitre 9).

Si votre ordinateur a des problèmes et vous craignez la présence d'un virus, reportez-vous à la section Diagnostic (chapitre 7). Nous vous indiquons brièvement comment dépanner votre ordinateur et déterminer s'il est réellement atteint d'un virus. Dans ce cas, suivez les instructions d'envoi des fichiers suspects au centre de recherche de virus d'Intego pour que nous puissions les inspecter.

2 - Introduction aux virus informatiques

Raisons de se protéger

Votre ordinateur contient des informations et des fichiers importants. Si vous les exploitez dans le cadre de votre activité professionnelle, vous devez avoir une idée du coût que la perte de ces fichiers entraînerait, aussi bien en temps qu'en argent. Même en tant qu'utilisateur particulier, vous avez certainement des fichiers que vous n'aimeriez pas perdre. Quoi qu'il en soit, si un virus devait effacer tous vos fichiers, si peu importants soient-ils, la réinstallation du système et de tous vos programmes vous prendrait beaucoup de temps.

Un programme antivirus est comparable à un contrat d'assurance. Naturellement, vous pouvez penser que votre ordinateur ne sera jamais infecté par un virus. Mais si cela arrive, vous risqueriez de vous en vouloir. Intego VirusBarrier X est votre assurance contre tous les types de virus – le programme veille sur votre ordinateur pour votre plus grande tranquillité.

La menace des virus est réelle. Le nombre de virus découverts quotidiennement ne cesse d'augmenter. Bien que les ordinateurs Macintosh soient relativement privilégiés par rapport aux systèmes sous Windows, il existe toujours un risque de voir des virus existants ou nouveaux s'infiltrer dans votre ordinateur et endommager vos fichiers.

Virus informatiques

Il n'y a rien qui puisse plus effrayer un utilisateur que d'insinuer que son ordinateur est peut-être atteint d'un virus. La surprise laisse souvent place à la

stupéfaction. En fait, les utilisateurs ont tous entendu parler des dégâts que pouvaient causer les virus. Même si ces histoires peuvent en faire sourire certains, personne en revanche ne peut rester indifférent en découvrant que son ordinateur est entaché d'un virus.

Avec le développement des communications et l'échange massif de fichiers par courrier électronique, les virus informatiques sont devenus une véritable menace. Un virus peut se propager aussi rapidement qu'une épidémie de grippe, et ce à partir d'un seul ordinateur. Qu'est-ce au juste qu'un virus informatique ? Comment fonctionne-il ? Pourquoi est-il si dangereux ?

C'est au début des année 1980, quand fut mis en circulation un programme informatique autoreproducteur, que le terme virus fut appliqué pour la première fois aux ordinateurs.

Un virus n'est rien d'autre qu'une séquence de code exécutable attachée à un fichier ou une application. Les virus ne s'attrapent pas dans l'air – il leur faut un moyen de transmission, tel qu'une disquette, un CD-ROM ou un fichier envoyé via Internet. À l'instar des virus qui envahissent notre organisme, les virus informatiques tentent de se reproduire après avoir infecté un hôte et s'attachent à d'autres fichiers et applications. Ils se reproduisent, attaquent de nouveaux hôtes, et ainsi de suite.

De fait, les virus sont de petits programmes informatiques – plus ils sont petits, plus ils sont redoutables, car ils se dissimulent plus facilement dans les fichiers et applications et échappent ainsi à la détection. Ils sont écrits dans un seul but : se reproduire et se propager aux autres ordinateurs. Bien que certains virus soient inoffensifs ou ne provoquent que l'apparition d'un message à l'écran, la plupart d'entre eux produisent des effets néfastes sur les ordinateurs et les fichiers. Même

s'il existe des exemples notables de virus écrits sans aucune intention de nuire, le plus souvent, le seul but de leurs auteurs est de détruire des fichiers et de transmettre ces virus à d'autres ordinateurs.

De l'ordinateur personnel à l'ordinateur de réseau d'entreprise, un virus informatique peut contaminer n'importe quel ordinateur, du moins si aucune précaution n'a été prise. La meilleure précaution que vous puissiez prendre est d'utiliser le programme Intego VirusBarrier X et, surtout, de veiller à le mettre à jour régulièrement.

Auteurs des virus

En dépit de ce que prétendent certaines personnes médisantes, les virus informatiques ne sont pas écrits par les éditeurs de programmes antivirus. Les virus en circulation leur donnent probablement suffisamment de mal sans qu'ils aient besoin de trouver d'autres occupations.

Personne ne sait réellement qui sont les auteurs de virus – des petits génies en crise d'adolescence, des pirates surdoués, qui peut le dire ?

Même s'il est vrai que certains auteurs de virus sont arrêtés, la proportion des arrestations demeure infime. D'autant que ceux qui se font démasquer cherchent peut-être aussi à se faire remarquer – bon nombre de virus contenaient le nom de leur auteur. D'autres sont simplement des vandales qui tirent un malin plaisir à voir les dommages que peuvent causer leurs programmes relativement simples. Et enfin ceux qui, par simple curiosité, créent des virus pour voir leur portée et l'étendue de leurs effets. À moins que les virus soient, comme l'a affirmé un auteur de virus, « une forme électronique de graffiti » ?

Il existe même des cas de virus dénués de « mauvaises intentions » qui ont fini par causer de nombreux problèmes. Le virus MacMag, dont le but initial était de diffuser un message de paix, en est un parfait exemple. (Pour plus de détails sur ce virus, reportez-vous au chapitre 9, Encyclopédie des virus.)

Depuis l'avènement d'Internet, la véritable crainte à propos des virus ne vient plus de ces individus isolés désireux de propager un virus juste pour se faire remarquer. Elle vient de véritables criminels informatiques dont le but est de faire subir des préjudices économiques de grande ampleur par le biais de virus. Les éclosions de virus, comme le virus LoveBug, ont démontré combien l'attaque pouvait s'avérer coûteuse pour une société en termes de productivité et de temps d'immobilisation. Voilà une raison suffisante pour justifier une protection efficace.

Mode de fonctionnement des virus informatiques

Dans l'esprit de la plupart des utilisateurs, le terme « virus informatique » englobe de nombreux types de « maliciels », dont certains ne sont pas des virus : par exemple, les chevaux de Troie et les vers fonctionnent de manière différente et ne se reproduisent pas systématiquement comme le font les virus. Pourtant, on a souvent tendance à les associer à la famille des virus. Bien que ces programmes soient malveillants et puissent gravement endommager votre ordinateur et vos fichiers, ils fonctionnent différemment.

Un vrai virus est une courte séquence de code informatique – autrement dit, des instructions de programmation – qui peut être exécutée ou mise en œuvre sur le type d'ordinateur visé. Ainsi, les virus conçus pour s'attaquer aux ordinateurs fonctionnant sous DOS et Windows n'ont aucun effet sur les ordinateurs Macintosh et vice versa. (Cela dit, si vous utilisez un de ces systèmes d'exploitation

sur votre Macintosh à l'aide d'un émulateur, vous devrez vous pencher sur la vulnérabilité du système d'émulation face aux virus dont ils sont la proie.)

Une fois activés sur l'ordinateur, les virus effectuent deux opérations. Ils essaient d'abord d'exécuter leur code afin de mener à bien leur mission destructrice, puis ils tentent de se reproduire en copiant ce code dans d'autres fichiers, applications, disques ou volumes de réseau. Voici un exemple des dégâts que pourrait causer un virus fictif sur votre Macintosh. (Le cas suivant présente les effets d'un cheval de Troie.)

> Un ami ou un client vous a envoyé un programme infecté via Internet. Bien que l'on vous ait conseillé de ne pas ouvrir de pièces jointes en provenance d'inconnus, vous décidez d'ouvrir le fichier estimant qu'il provient d'une source sûre. Supposons qu'il s'agisse d'une application, par exemple, une carte de vœux animée. Vous double-cliquez sur le fichier et l'application commence à s'exécuter. Mais au cours de son exécution, elle délivre sa signature virale et modifie votre fichier Système. Elle copie le code parasite dans votre Système et, par la même occasion, recherche d'autres fichiers Système sur le réseau local de votre société pour s'y copier également. Une fois la présentation terminée, vous quittez l'application. Vous n'avez encore rien remarqué d'anormal sur votre ordinateur, car le code a été défini de manière à ne produire ses effets qu'au redémarrage de l'ordinateur.
>
> Le lendemain matin, vous vous apprêtez à entamer votre journée de travail et démarrez votre ordinateur, mais vous remarquez qu'il est plus long à démarrer que d'habitude. Lorsqu'il a enfin démarré, vous trouvez qu'il fonctionne très lentement. Vous allez pour ouvrir le rapport urgent à terminer avant le déjeuner et constatez que le fichier a disparu. Vous parcourez le disque dur et découvrez avec effroi que des dizaines, voire des

centaines de fichiers ont disparu. C'est alors que vous réalisez que la veille, vous avez oublié d'accomplir une sauvegarde de votre disque dur et que vous n'avez aucune copie de ces fichiers.

Vous avez déjà envoyé cette carte de vœux animée à d'autres amis, mais vous n'avez pas établi de rapport entre cette carte et la disparition de vos fichiers. Ce n'est que quelques heures plus tard, quand l'un de vos amis vous apprend que la carte de vœux animée a affecté son ordinateur, que vous prenez conscience de ce qui s'est passé.

Comme le montre cet exemple, une simple infection de virus peut avoir de graves conséquences. Non seulement pour vous, mais aussi pour vos correspondants. L'un des grands problèmes liés aux virus vient de l'échange constant de fichiers via Internet, les ordinateurs risquent de s'infecter beaucoup plus rapidement que par le passé, à l'époque de la transmission des fichiers principalement par disquettes. En vous protégeant avec Intego VirusBarrier X, vous protégez aussi les autres.

Quiconque regarde les nouvelles ou lit la presse a sans doute entendu parler des derniers cas de virus informatiques qui, en moins de 24 heures, ont parcouru le monde entier. Bien que les virus perfectionnés que sont Melissa et Love Bug aient affecté des systèmes Windows équipés de logiciels spécifiques, rien ne permet d'affirmer que des virus comparables ne s'attaqueront jamais aux ordinateurs Macintosh.

Différents types de virus

On peut diviser les virus en deux types différents, selon les éléments de l'ordinateur auxquels ils s'attaquent. Les virus du premier type sont appelés virus système, car ils s'attaquent au fichier Système, aux extensions ou au fichier Desktop. Les virus du deuxième type, appelés virus de fichiers, infectent les applications, les fichiers de données, voire les tableaux de bord et les extensions.

Virus système

Les virus système sont les plus dangereux de tous, car ils sont capables d'endommager le système d'exploitation lui-même. On associe également à cette catégorie deux autres types de maliciels : les chevaux de Troie et les vers. Bien qu'ils soient techniquement différents des virus système, leur champ d'action tend à être plus global que celui des virus de fichiers.

Virus

Un virus informatique est un petit programme qui agit comme un parasite. Vivant dans un fichier hôte ou un programme, il est capable d'infecter les fichiers et les applications, de se reproduire et de se propager à d'autres ordinateurs par le biais des fichiers et des applications infectés. Il n'est guère surprenant que l'on utilise des termes habituellement appliqués aux maladies pour parler des virus informatiques : ils œuvrent d'une manière très comparable.

Les virus qui s'attaquent au système sont parmi les plus destructeurs. Les dégâts qu'ils peuvent causer sont tels que la réinstallation complète du système et même le reformatage du disque dur peuvent s'avérer nécessaires, tout comme la vérification de toutes les sauvegardes pour s'assurer qu'elles sont saines.

Certains de ces virus, tels que les virus CDEF ou WDEF, n'infectent que les fichiers Desktop du Macintosh (sur les versions Mac OS 9 et antérieures). Ce sont des fichiers invisibles capables d'identifier la parenté entre les icônes et les fichiers et applications. Bien que n'affectant pas d'autres fichiers, ils se propagent très rapidement, du fait que votre Macintosh lit ces fichiers Desktop dès le montage d'un disque ou volume.

D'autres virus système, tels que certaines variantes du virus SevenDust, peuvent infecter les fichiers Système, les tableaux de bord et les applications et, à une date et une heure précises, supprimer tous les fichiers non applicatifs présents sur votre disque de démarrage.

Certains virus agissent très rapidement, d'autres sont programmés pour se manifester à un moment déterminé. Certains se contentent uniquement de se propager à d'autres disques et volumes, mais tous les virus système sont potentiellement dangereux.

Chevaux de Troie

Le nom « Cheval de Troie » est tiré d'un épisode de la guerre qui opposa les Grecs et la cité de Troie il y a plus de deux mille ans. C'était un cheval de bois gigantesque et creux que les Grecs édifièrent et donnèrent soi-disant en cadeau aux Troyens en vue de terminer la guerre. Bien que ce geste laissât certains Troyens

perplexes, le cheval fut amené à l'intérieur de leur forteresse. La même nuit, les guerriers grecs sortirent du cheval, ouvrirent les portes de la cité et les troupes grecques stationnées à l'extérieur la prirent d'assaut.

Bien sûr, personne n'a jamais conseillé aux Troyens de ne pas ouvrir les pièces jointes. Les chevaux de Troie dont on se préoccupe aujourd'hui sont des programmes apparemment inoffensifs, prétendant exécuter certaines tâches mais qui, en fait, contiennent un code parasite ou des virus. Dans de nombreux cas, les chevaux de Troie sont potentiellement plus dangereux que les autres virus. Ce fut notamment le cas de ChinaTalk, qui ressemblait à une extension système mais qui supprimait les dossiers, ou du célèbre cheval de Troie MacMag, qui infectait les fichiers Système.

Vers

Les vers constituent la forme la plus ancienne des programmes informatiques parasites. Ils se propagent autrement que par attachements aux fichiers et aux applications, et leur identification peut être très difficile. AutoStart, le plus récent des vers à affecter les Macintosh, crée des fichiers invisibles qui peuvent détruire les données et les fichiers.

Les vers se propagent en utilisant les fonctions du Mac OS. Par exemple, le vers AutoStart se propage à partir de CD-ROM infectés en utilisant la fonction Lecture automatique de Mac OS. Il crée des extensions invisibles qui s'activent à chaque redémarrage de l'ordinateur.

Virus de fichiers

Les virus de fichiers diffèrent des virus système car ils s'attachent aux fichiers de données, plutôt qu'aux applications, et leurs hôtes ont besoin de programmes spécifiques pour produire leurs effets destructeurs. Parmi les derniers virus de fichiers à avoir menacé les ordinateurs Windows, on peut citer les très virulents Melissa et LoveBug ; ils étaient transmis sous forme de pièces jointes qui, une fois ouvertes, activaient certaines fonctions intégrées aux applications Microsoft pour Windows. D'une certaine manière, on pourrait penser que ces virus étaient des chevaux de Troie. Or, à la différence des chevaux de Troie qui se présentent comme des applications capables d'accomplir certaines tâches, ces virus de fichiers n'étaient rien d'autre que du code incorporé à des fichiers.

Les Macro virus

La plupart des virus de fichiers sont des macro virus. Cette famille de virus constitue aujourd'hui la plus grande menace pour les utilisateurs d'ordinateurs Macintosh.

Le premier véritable macro virus découvert fut le virus Concept, qui s'attaquait aux fichiers Microsoft Word. D'autres variantes lui emboîtèrent rapidement le pas, les concepteurs de virus ayant compris que l'ubiquité de ce programme présentait un potentiel destructeur remarquable. Plus tard, des macro virus allaient être écrits pour exploiter également Microsoft Excel. En l'espace de 5 ans après l'apparition de ce premier virus, plusieurs milliers de macro virus allaient être découverts.

Le véritable danger des macro virus vient du fait qu'il s'agit des premiers virus multi-plates-formes. Pendant des années, les utilisateurs de Macintosh pouvaient s'estimer à l'abri des virus, sachant que seules quelques dizaines de virus menaçaient les ordinateurs Macintosh, contre plusieurs milliers pour Windows. Cependant, avec la forte dissémination des macro virus, le danger est bien réel.

De nombreux programmes offrent la possibilité de créer des macro-commandes. Ces petits programmes utilisent les fonctions internes d'une application, telle que AppleWorks, pour « enregistrer » et « lire » des séquences de commandes souvent utilisées. D'autres applications, comme Nisus Writer, offrent un langage macro plus puissant combinant des commandes de menus et un langage de programmation. Les fonctions macro de programmes tels que Microsoft Word et Excel sont basées sur le langage Visual Basic de Microsoft, qui s'apparente au langage de programmation Basic.

Si les auteurs de macro virus prennent souvent pour cible les programmes Microsoft, c'est en partie parce que ces applications permettent l'ajout de macros dans les fichiers de données. Par le passé, on craignait uniquement les virus transmis par les applications, car pour entrer en action, un virus doit s'exécuter et seules les applications le permettaient. Mais l'approche de Microsoft Visual Basic est différente – si vous souhaitez utiliser une macro, vous pouvez soit l'exécuter à partir de votre modèle, soit l'ajouter à un fichier de données. Au début, les utilisateurs furent surpris, car ils pensaient que rien ne s'exécutait lors de l'ouverture d'un fichier de traitement de texte ou de tableur. Mais ces fichiers peuvent en fait contenir des « programmes » et accomplir des choses insoupçonnables.

Comme le langage macro permet de modifier des fichiers, un macro virus peut se copier dans d'autres fichiers utilisés par la même application ; il risque donc de se propager lors de l'ouverture, la création ou la transmission de fichiers.

La majorité des macro virus ayant pour cible les fichiers Microsoft Word utilisent des commandes telles que AutoOpen, AutoClose, AutoExec et AutoExit. Ces commandes s'exécutent lorsqu'un certain événement intervient dans le fichier, et ces quatre événements se produisent à chaque utilisation de fichier. Une macro, écrite pour se copier uniquement à l'exécution d'une certaine commande, aurait moins de chances de se propager.

De manière générale, les macro virus agissent à l'ouverture d'un fichier en se copiant dans le modèle qui s'est également ouvert. Ce modèle, vous ne l'avez pas ouvert à proprement parler. De fait, il est toujours ouvert en tâche de fond – il contient certaines informations de personnalisation, telles que des barres d'outils, ainsi que les macros légitimes éventuellement ajoutées.

Le macro virus type qui affecte Microsoft Word se copie dans le modèle actif, modifie certains éléments de menu de manière que vous ne puissiez pas modifier le modèle, change les types de fichier (leurs icônes sont modifiées, devenant elles-mêmes des modèles), puis se copie à partir du modèle corrompu dans tous les nouveaux fichiers créés ou ouverts. Ce virus peut être supprimé s'il est détecté à temps. Il suffit de supprimer le fichier modèle actif et les fichiers infectés.

D'autres macro virus risquent d'être beaucoup plus dangereux. Ils peuvent endommager ou supprimer vos fichiers, masquer certaines fonctions d'applications, et plus encore. Pour couronner le tout, ce sont des virus multi-plates-formes qui endommagent aussi bien les ordinateurs Macintosh que les PC fonctionnant sous Windows.

Il importe de noter que les langages macro sont des outils très puissants et potentiellement très utiles. Toutes les macros ne sont pas des virus. La fonction de Microsoft Word alertant de la présence d'une macro dans les documents n'incite guère à utiliser la fonction macro. Le problème vient du stockage des macros dans les fichiers de données. Si elles étaient stockées dans des fichiers distincts (cas de certaines applications, telles que Nisus Writer), les utilisateurs pourraient échanger des macros avec l'assurance que les fichiers ouverts ne contiennent que des données. Malheureusement, ce principe de stockage en fichier de données entraîne trop de méfiance face aux macros, au lieu de tirer profit de leurs propriétés amélioratrices des fonctions.

Intego VirusBarrier X détecte tous les macro virus connus de Microsoft Word et Excel ; il est mis à jour dès la découverte de nouveaux macro virus.

Canulars

Les canulars, c'est-à-dire les messages électroniques ou les articles de groupes de nouvelles (ou « newsgroups ») diffusés pour avertir à tort les internautes de l'existence de virus informatiques, sont un problème croissant. Bien qu'il ne s'agisse pas de virus à proprement parler, ils ont tendance à se reproduire de la même manière – pensant bien faire, les utilisateurs inquiets font suivre ces messages à leurs amis et collègues, causant ainsi des craintes injustifiées à propos de virus imaginaires.

Un des canulars les plus répandus se nomme Good Times. Ce « virus » tire son nom de l'objet du message électronique censé contenir un virus. On serait tenté de penser qu'un tel canular est voué à une existence éphémère. Or, le message du virus Good Times continue toujours de circuler depuis son apparition en 1994.

D'autres messages de ce type circulent régulièrement sur Internet, et il est probable que vous en ayez déjà rencontré un, voire plusieurs.

Ces canulars s'appuient sur le manque de connaissances informatiques de beaucoup d'internautes. Il est vrai que ces messages revêtent toujours un caractère sérieux et semblent parfois émaner de grandes sociétés informatiques. Pourtant, ce ne sont que des plaisanteries, somme toute, d'un goût très douteux.

Si vous recevez un message de ce type et craignez qu'il s'agisse non pas d'un canular mais d'une véritable alerte de virus, la première chose à faire est de contacter votre administrateur système pour déterminer si vos craintes sont justifiées, si vous travaillez dans une société. Si vous êtes un particulier, n'hésitez pas à consulter le site Web d'Intego à l'adresse suivante : www.intego.com. Dès que nous apprenons l'existence de nouveaux virus, nous y diffusons un message d'alerte dans les meilleurs délais. Le centre de recherche de virus d'Intego fonctionne 24H/24, 7 jours sur 7 et réagit aux premiers signes d'apparition de nouveaux virus.

Si vous pensez avoir contracté un nouveau virus, reportez-vous au chapitre 7 pour savoir comment analyser votre ordinateur et contacter le centre de recherche de virus d'Intego.

Modes de propagation des virus

Les virus se propagent de diverses manières ; ils ne peuvent se propager que via deux éléments : les fichiers ou les supports de stockage. Dans le cas du Macintosh, les supports amovibles, tels que les CD-ROM ou les cartouches Zip, contiennent des fichiers invisibles appelés fichiers Desktop. Ces fichiers renferment des

informations destinées au Système, concernant les icônes de fichiers et les applications. Les virus qui s'attaquent aux fichiers Desktop peuvent se propager pendant que l'ordinateur lit ces supports amovibles. En effet, le Macintosh lit ces fichiers dès le montage d'un disque ou d'un volume. Intego VirusBarrier X protège votre ordinateur en analysant les supports amovibles, avant même que les virus aient l'occasion de se propager. Si Intego VirusBarrier X détecte un virus dans ces fichiers Desktop, il les désinfecte avant que l'ordinateur ne les lisent.

Les virus peuvent également se propager par l'intermédiaire de fichiers infectés. Ces fichiers peuvent résider sur des CD-ROM et autres supports amovibles ou être téléchargés sur Internet. Ils peuvent être envoyés en pièces jointes par courrier électronique. Les fichiers infectés ne peuvent pas libérer leurs virus tant qu'ils n'ont pas été ouverts ou lus. Vous ne risquez donc pas de propager un virus par simple copie d'une application. Seule l'exécution de l'application vous expose à ce risque. Il en va de même pour les fichiers de données – si vous recevez un fichier contenant un macro virus, vous n'avez rien à craindre tant que vous n'ouvrez pas ce fichier. Intego VirusBarrier X protège l'ordinateur contre ces virus en analysant les fichiers à l'écriture, l'utilisation ou l'ouverture. Dès que vous manipulez un fichier, celui-ci est aussitôt analysé. Si Intego VirusBarrier X détecte un virus, le fichier ou l'application est désinfecté ou rendu inexploitable.

Modes de protection possibles contre les virus

Pour vous prémunir contre les virus informatiques, il vous suffit d'appliquer quelques règles simples. La première, et certainement la plus importante, est d'utiliser Intego VirusBarrier X. Votre ordinateur est alors constamment surveillé et les virus sont recherchés automatiquement. Intego VirusBarrier X constitue la

meilleure protection pour votre Macintosh ; il œuvre en tâche de fond pour assurer la sécurité de votre ordinateur.

Pour rester protégé contre les nouveaux virus, vous devez mettre à jour Intego VirusBarrier X de façon régulière. La fonction NetUpdate du programme simplifie cette opération. Nous vous recommandons d'exécuter cette fonction de mise à jour au moins une fois par mois. Vous pouvez même de temps à autre consulter le site Web d'Intego (www.intego.com) pour voir s'il existe de nouvelles mises à jour contre des virus récemment découverts.

Un autre principe de base est d'utiliser uniquement des logiciels provenant de sources sûres. Les logiciels piratés peuvent contenir des virus ou même un cheval de Troie inattendu. Veillez à n'installer que les logiciels dont vous connaissez la provenance. Intego VirusBarrier X vous protège en contrôlant chacun des fichiers installés, vérifiant qu'ils sont sains.

Par ailleurs, vous devez faire preuve de la plus grande vigilance en ce qui concerne les fichiers reçus par courrier électronique ou via Internet. On a vu à travers l'exemple du cheval de Troie combien l'ouverture candide d'une pièce jointe pouvait être périlleuse. On avait l'habitude de dire qu'il ne fallait jamais ouvrir de pièces jointes provenant d'inconnus. Or, les derniers virus contractés par des ordinateurs Windows se sont propagés par l'envoi de pièces jointes entre amis et collègues de travail. Quoi qu'il en soit, si vous recevez une pièce jointe de quelqu'un d'inconnu, évitez de l'ouvrir. Cela ne garantit pas pour autant que vos collègues ne transmettent pas involontairement des virus dans leurs fichiers. Intego VirusBarrier X vous protège en analysant chaque fichier ouvert et en éliminant automatiquement tous les virus connus. Si vous travaillez sur un ordinateur en réseau et Intego VirusBarrier X détecte un virus dans une pièce

jointe, veillez à contacter immédiatement votre administrateur réseau afin qu'il supprime le fichier infecté du serveur de messagerie de l'entreprise.

Bien qu'Intego VirusBarrier X offre un niveau de protection antivirale élevé, la protection de vos données exige que vous appliquiez une autre règle : sauvegarder régulièrement vos fichiers. Vous devez non seulement sauvegarder les fichiers importants tous les jours, mais également en faire plusieurs sauvegardes. En effet, le support de sauvegarde peut s'endommager ou s'altérer et les sauvegardes ne seraient plus d'aucun secours. Intego Personal Backup X offre une solution complète de sauvegarde, le logiciel sait même effectuer des sauvegardes automatiques, vous êtes assuré de toujours disposer d'une copie saine de vos données au cas où votre Mac attraperait un virus.

Nous vous conseillons une bonne méthode de travail : si vous sauvegardez vos fichiers à l'aide d'un lecteur Zip, utilisez au moins deux cartouches Zip, en opérant un roulement quotidien entre les deux supports. C'est une simple assurance. Non seulement vous serez assuré d'avoir des copies saines de vos fichiers dans le cas où vous trouveriez un virus sur votre ordinateur, mais vos données seront à l'abri d'autres types de problèmes, tels que des blocages de disque dur, etc.

Compte tenu du coût relativement modique des supports amovibles ou même des CD-ROM inscriptibles et des disques durs externes, vous pouvez également sauvegarder votre Système et vos applications, d'autant que vous n'avez pas besoin de répéter cette opération aussi souvent. Soyez vigilant ! Si, pour quelque raison que ce soit, l'ordinateur se corrompt, la réinstallation du système et des applications vous prendra beaucoup de temps. Si, en revanche, vous avez sauvegardé l'ordinateur en intégralité, cette opération ne prendra que quelques minutes.

3 - Installation

Configuration matérielle et logicielle requise

- Tout ordinateur compatible Mac OS X (supporté officiellement par Apple)
- Mac OS X 10.1.1 ou ultérieur, ou Mac OS X Serveur 10.1.1 ou ultérieur
- 20 Mo d'espace libre sur disque dur
- Résolution d'écran minimum 800 x 600

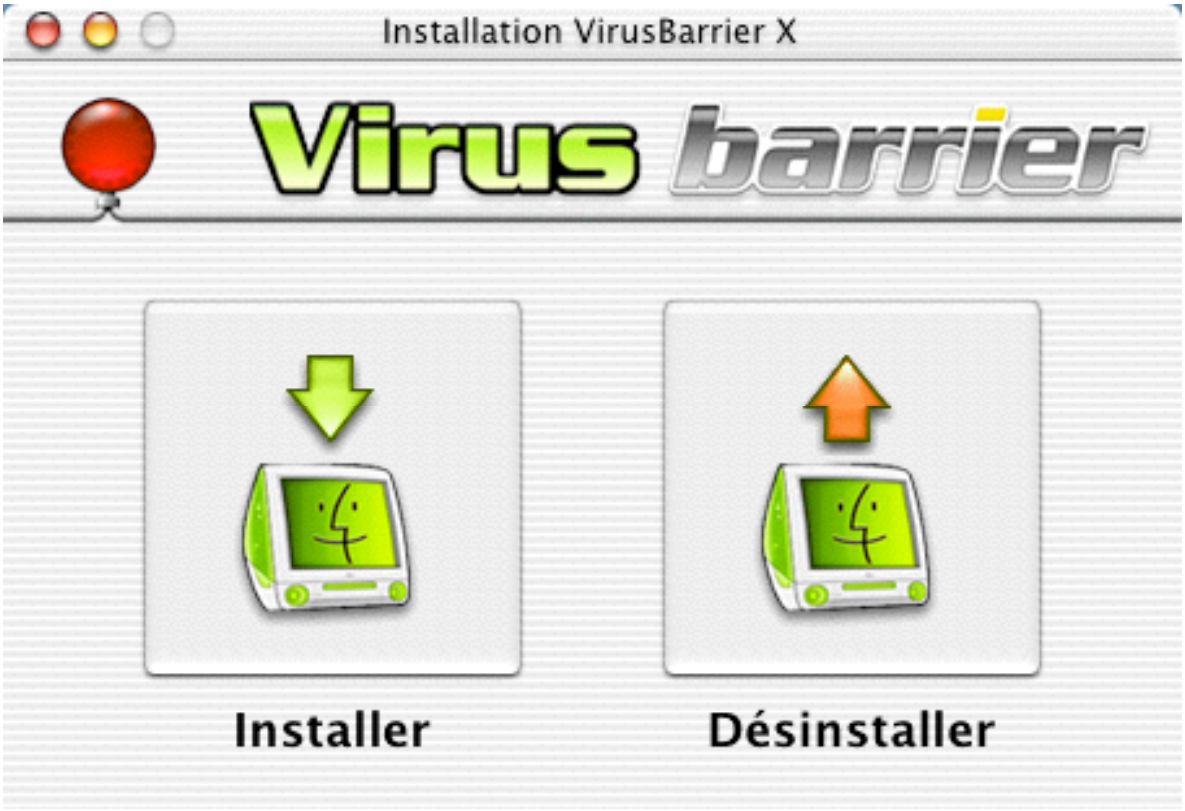
Installation d'Intego VirusBarrier X

L'installation d'Intego VirusBarrier X est très simple. Insérez le CD-ROM Intego VirusBarrier X dans le lecteur de CD-ROM de votre ordinateur. La fenêtre qui apparaît contient l'installeur d'Intego VirusBarrier X, le fichier Lisez-moi, le manuel Intego VirusBarrier X (ce fichier) et un installeur d'Acrobat Reader. (Si vous avez acheté Intego VirusBarrier X par téléchargement, un fichier disque image apparaît, appelé Intego VirusBarrier X Install.dmg. Double-cliquez sur ce fichier pour ouvrir l'image disque, qui montera sur le bureau.)

Tout d'abord, consultez le fichier Lisez-moi, pour les changements de dernière minute.

Puis double-cliquez sur l'installeur d'Intego VirusBarrier X.

La fenêtre de l'installeur propose deux options : Installer et Désinstaller.



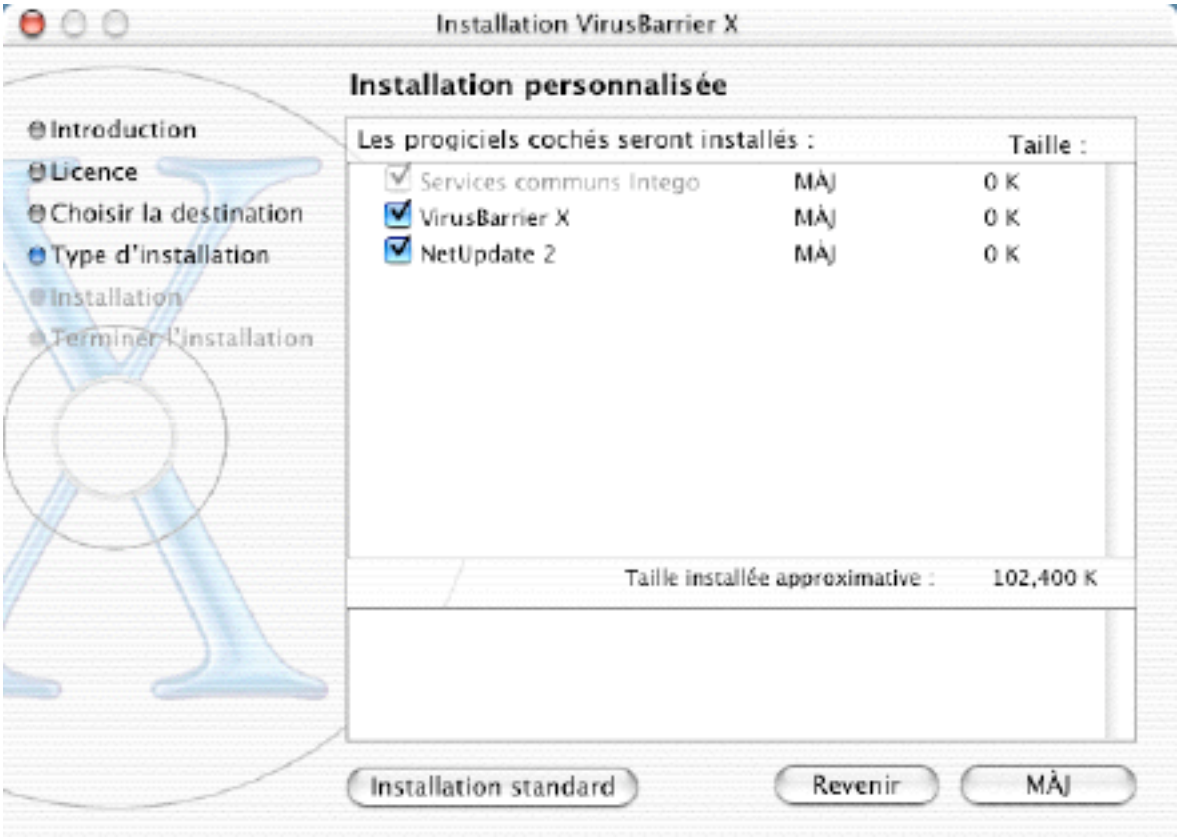
Cliquez sur Installer pour l'installation d'Intego VirusBarrier X. Si vous avez besoin de désinstaller le programme, utilisez le bouton Désinstaller.

Une fenêtre apparaît, vous informant de la nécessité d'entrer un mot de passe administrateur pour installer Intego VirusBarrier X. Cliquez sur le cadenas, pour entrer votre mot de passe, ou entrez le mot de passe dans le dialogue qui apparaît (OS X 10.2 ou ultérieur). Entrez le mot de passe et cliquez sur OK. La fenêtre suivante apparaît :

Cliquez sur Continuer pour la suite de l'installation. La fenêtre contenant la licence d'Intego VirusBarrier X apparaît. Cliquez sur Continuer, et, si vous en acceptez le contenu, cliquez sur Accepter ; sinon, cliquez sur Refuser, et l'installeur va quitter.

La fenêtre suivante présente tous les disques ou volumes disponibles sur l'ordinateur. Choisissez le disque ou le volume où vous souhaitez installer Intego VirusBarrier X, puis cliquez sur Continuer.

Cliquez sur Installer pour une installation de base du logiciel. Si vous souhaitez une installation personnalisée, cliquez sur Personnaliser. La fenêtre suivante apparaît :

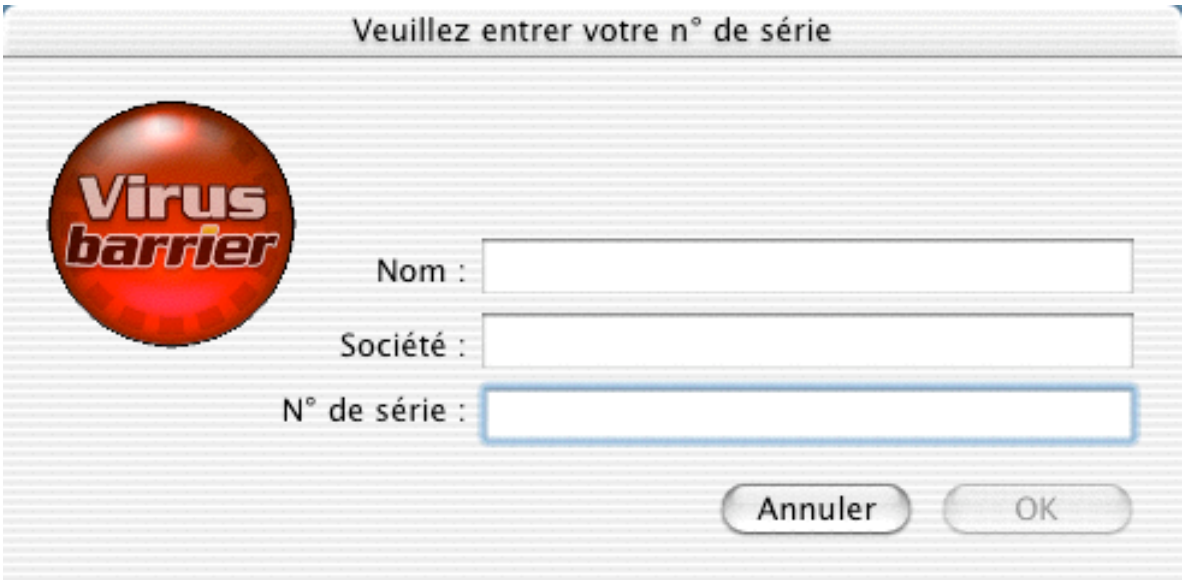


Cette fenêtre vous propose de choisir les éléments à installer. Notez que la case **Services communs Intego** est grisée, leur installation étant systématique. Vous avez le choix d'installer Intego VirusBarrier X et/ou NetUpdate. Si des programmes d'Intego sont déjà installés sur votre ordinateur, l'option de Mise à niveau de l'installation (bouton MÀJ) est proposée – cela signifie que certains composants utilisés par tous les programmes d'Intego ne seront pas réinstallés.

Vous devez redémarrer l'ordinateur après la procédure d'installation.

Enregistrement d'Intego VirusBarrier X

Quand vous redémarrez l'ordinateur, ouvrez Intego VirusBarrier X - il se trouve dans le dossier Applications. Intego ouvre son programme d'enregistrement et la fenêtre suivante apparaît :



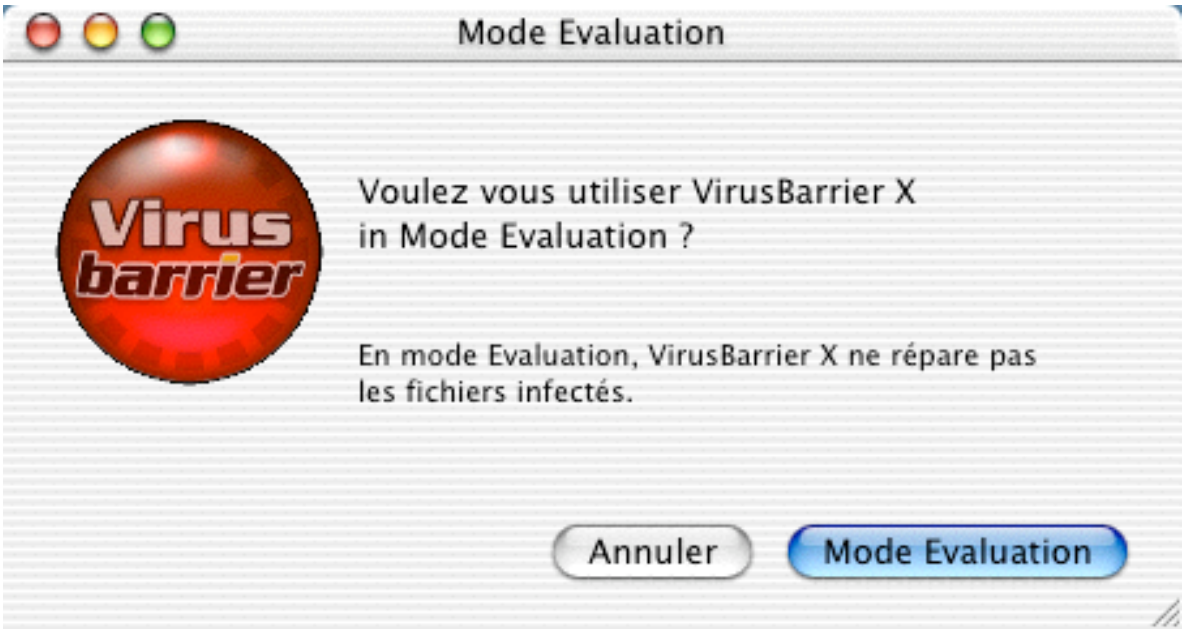
Comme Mac OS X est un système d'exploitation multi-utilisateurs, tous les utilisateurs n'ont pas les mêmes autorisations. Au tout premier démarrage de Intego VirusBarrier X, tout utilisateur peut entrer le numéro de série, mais seul un utilisateur ayant les autorisations d'administrateur peut configurer le programme.

Vous devez entrer votre nom, le nom de votre société, le cas échéant, et votre numéro de série. Ce numéro se trouve sur un autocollant au dos du boîtier du CD

d'Intego VirusBarrier X. Une fois l'enregistrement terminé, Intego VirusBarrier X s'ouvre et vous pouvez configurer le programme, si vous êtes un administrateur.

Mode d'évaluation d'Intego VirusBarrier X

Intego VirusBarrier X propose un mode d'évaluation, permettant de découvrir le fonctionnement du programme avant l'achat. Pour utiliser Intego VirusBarrier X en mode d'évaluation, cliquez sur Annuler quand la fenêtre d'enregistrement apparaît. L'écran vous demande de confirmer le choix du fonctionnement en mode d'évaluation. Pour cela, cliquez sur Mode Évaluation ; sinon, cliquez sur Annuler.


Mode Evaluation
Virus barrier
Voulez vous utiliser VirusBarrier X in Mode Evaluation ?
En mode Evaluation, VirusBarrier X ne répare pas les fichiers infectés.
Annuler
Mode Evaluation

4 - Prise en main rapide

Mode par défaut d'Intego VirusBarrier X

Dès que vous avez installé Intego VirusBarrier X, il commence automatiquement à surveiller votre ordinateur. Intego VirusBarrier X est conçu pour être simple et non-intrusif, et il protège totalement votre ordinateur sans que vous ayez à intervenir.

Une fois le programme installé, vous pouvez simplement le laisser fonctionner de manière indépendante. Cependant, nous vous conseillons de régler NetUpdate pour qu'il vérifie automatiquement la présence de mises à jour du programme, ou de le faire manuellement au moins une fois par mois.

Pour ouvrir Intego VirusBarrier X, modifier les réglages ou effectuer une analyse manuelle, double-cliquez sur l'icône d'Intego VirusBarrier X dans le dossier Applications.

Interface d'Intego VirusBarrier X

L'application Intego VirusBarrier X a l'interface suivante. Elle contient l'Orbe, le bouton de contrôle contextuel, ainsi que d'autres boutons, pour le choix des réglages et le lancement des analyses. Pour l'accès aux fonctions d'Intego VirusBarrier X, cliquez sur l'un des boutons de l'interface et son tiroir s'ouvre.

Orbe d'IntegoVirusBarrier X
Informations sur l'opération en cours.

Bouton de contrôle contextuel
Ce bouton change selon la fonction, telle que Analyser, Pause, Stop, etc.

Bouton Choisir
Choix du volume, du dossier ou du fichier à analyser à la recherche de virus.

Bouton Rapport
Ouverture de la liste des rapports, présentant les dates et heures des analyses manuelles et les fichiers infectés ou corrompus détectés.

Bouton NetUpdate
Ce bouton permet la vérification des mises à jour d'Intego VirusBarrier X.

Bouton Préférences
Choix des réglages de Intego VirusBarrier X.

Bouton i
Informations concernant Intego VirusBarrier X.

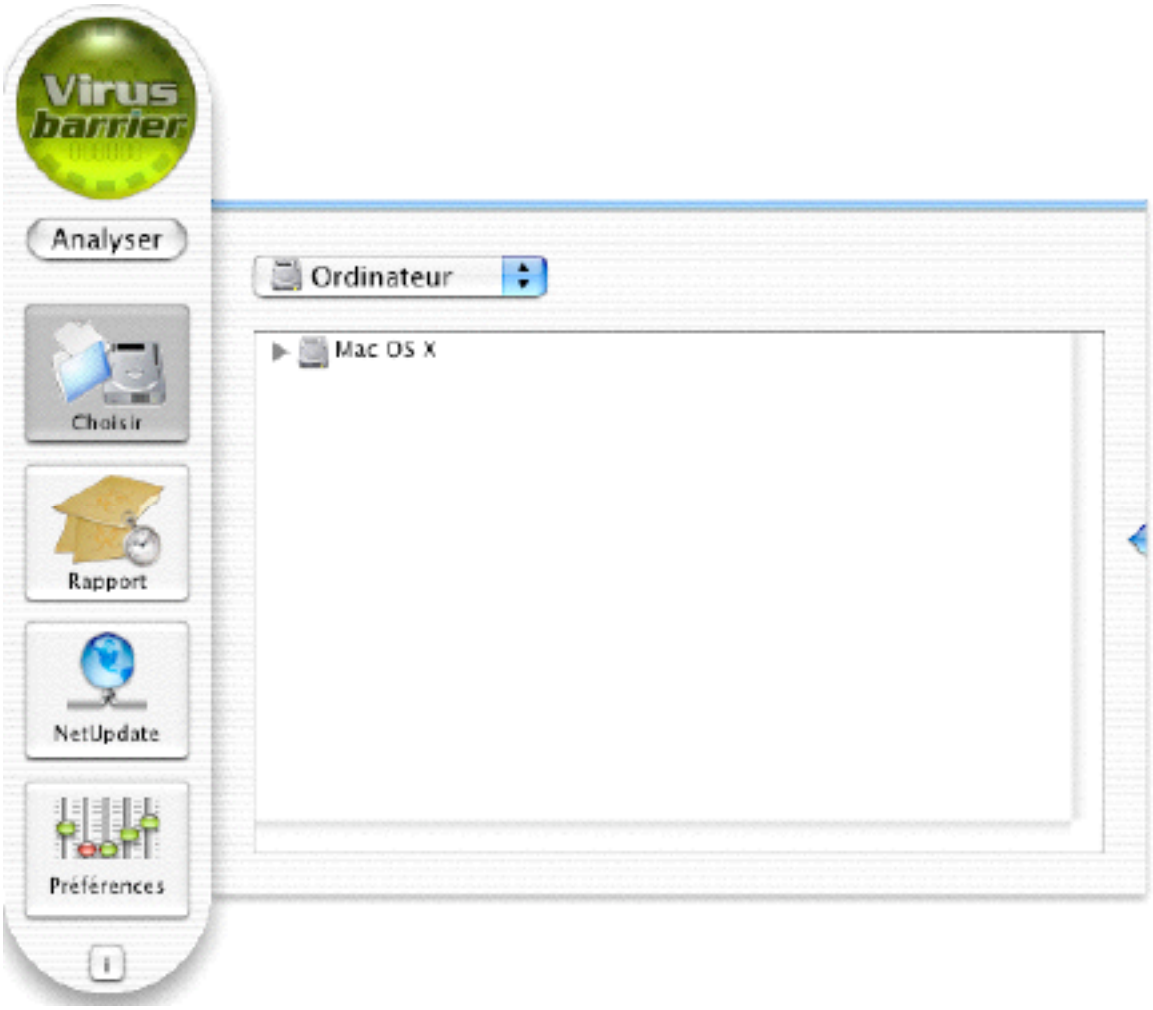
Pour fermer ce tiroir, cliquez sur son bouton ou sur le triangle situé à droite du tiroir. Vous pouvez également cliquer sur un deuxième bouton, ce qui fermera le premier tiroir et ouvrira le tiroir correspondant.

Lancement d'une analyse manuelle

Dès son installation, Intego VirusBarrier X surveille vos fichiers et assure qu'ils sont à l'abri des virus. Mais Intego VirusBarrier X vérifie également les fichiers au moment de leur lecture, de leur traitement ou de leur écriture. La procédure d'installation vous propose l'option d'exécuter une analyse manuelle immédiate de tous vos fichiers, pour s'assurer du nettoyage de tout votre ordinateur. Nous vous conseillons de passer par cette étape, pour vous assurer de l'absence de fichiers infectés. Ensuite, Intego VirusBarrier X s'assure que tous les nouveaux fichiers sont débarrassés des virus.

Si vous n'avez pas choisi de lancer une analyse complète dès l'installation, ou si vous souhaitez le faire manuellement à tout moment, ouvrez Intego VirusBarrier X en double-cliquant sur son icône dans le dossier Applications.

Cliquez sur le bouton Choisir, et le tiroir s'ouvre présentant tous les volumes montés sur votre ordinateur. Cette vue est de type liste du Finder, les volumes, les dossiers et les fichiers étant classés selon leur hiérarchie. Pour ouvrir un volume ou un dossier et en visualiser le contenu, cliquez sur le triangle à sa gauche ; tous les fichiers et dossiers seront listés au-dessous. Pour fermer un volume ou un dossier ouvert, cliquez sur ce même triangle.



Pour lancer l'analyse manuelle d'un volume, dossier ou fichier, double-cliquez sur l'élément choisi, ou cliquez une fois pour le sélectionner, puis cliquez sur le bouton Analyser. Vous constaterez le début de l'analyse d'après l'activité dans l'Orbe. Il indique d'abord le nombre de fichiers analysés en cours.

Si vous avez choisi Fichiers restant à analyser dans les Préférences, Intego VirusBarrier X compte le nombre de fichiers à analyser, puis affiche le nombre de fichiers restant à analyser et le pourcentage d'analyse restante. Si vous cliquez sur

l'Orbe, l'affichage est modifié et indique le nombre de fichiers analysés et le pourcentage correspondant.

Vous pouvez arrêter l'analyse à tout moment en appuyant sur le bouton Stop. Pour suspendre l'analyse, maintenez la touche Maj de votre clavier enfoncée, vous verrez que le bouton Stop devient Pause. Cliquez sur ce bouton et l'analyse marque un temps de pause.

Pour reprendre l'analyse, cliquez sur ce bouton, qui affiche alors Continuer.

Réglages de NetUpdate

Si vous cliquez sur le bouton NetUpdate, le tiroir correspondant s'ouvre. Ce tiroir permet la vérification des mises à jour, donne des informations sur la date de la dernière interrogation, le numéro de version d'Intego VirusBarrier X, et la date d'échéance de votre abonnement. Vous avez accès aux mises à jour du programme et des définitions de virus pendant un an à compter de la date d'achat d'Intego VirusBarrier X.

La mise à jour régulière d'Intego VirusBarrier X est très importante, pour vous assurer de la protection contre les virus les plus récents. Intego VirusBarrier X inclut NetUpdate, qui peut vérifier automatiquement la mise à jour éventuelle du programme, et la télécharger.

Pour rechercher les mises à jour, cliquez sur le bouton Interroger maintenant…. Intego NetUpdate s'ouvre et se connecte au serveur d'Intego à la recherche des mises à jour du programme ou des définitions de virus. Vous avez accès aux mises à jour du programme et des définitions de virus pendant un an à compter de la date d'achat d'Intego VirusBarrier X.

Vous pouvez régler NetUpdate, pour le choix des date et heure des mises à jour automatiques, dans le Panneau des Préférences NetUpdate sous les Préférences Système.

Pour en savoir plus sur NetUpdate, reportez-vous au chapitre 6, Réglages d'Intego VirusBarrier X et consultez le manuel NetUpdate.

Analyse en glisser-déposer

Vous pouvez également analyser un volume, un dossier ou un fichier en le faisant glisser sur n'importe quelle partie de l'interface d'Intego VirusBarrier X. Dès que vous le relâchez, Intego VirusBarrier X commence à l'analyser, comme c'est le cas pour toute analyse manuelle.

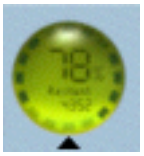
Utilisation d'Intego VirusBarrier X dans le Dock

Après l'ouverture, l'icône d'Intego VirusBarrier X apparaît dans le Dock.

Si vous cliquez sur cette icône, et choisissez Maintenir dans le Dock dans le menu déroulant, l'icône reste dans le Dock, même après que vous ayez quitté l'application.

L'icône Intego VirusBarrier X est verte quand l'application est ouverte, et rouge quand elle est fermée.

À tout moment, vous pouvez faire glisser des fichiers, dossiers ou volumes sur l'icône Intego VirusBarrier X dans le Dock, et Intego VirusBarrier X ouvre l'application et commence l'analyse des fichiers. L'Orbe indique l'état de l'analyse en cours dans le Dock.



Si vous cochez Masquer l'application au démarrage dans les Préférences, l'application Intego VirusBarrier X ne sera pas visible, et toute l'activité sera indiquée dans l'Orbe sur le Dock. Pour en savoir plus sur les préférences, reportez-vous au chapitre 6, Réglages d'Intego VirusBarrier X.

5 – Fonctions d'Intego VirusBarrier X

Intego VirusBarrier X est un programme puissant et convivial conçu pour protéger votre ordinateur contre tous les types de virus. Il opère en tâche de fond et vous offre une protection continue, efficace et silencieuse.

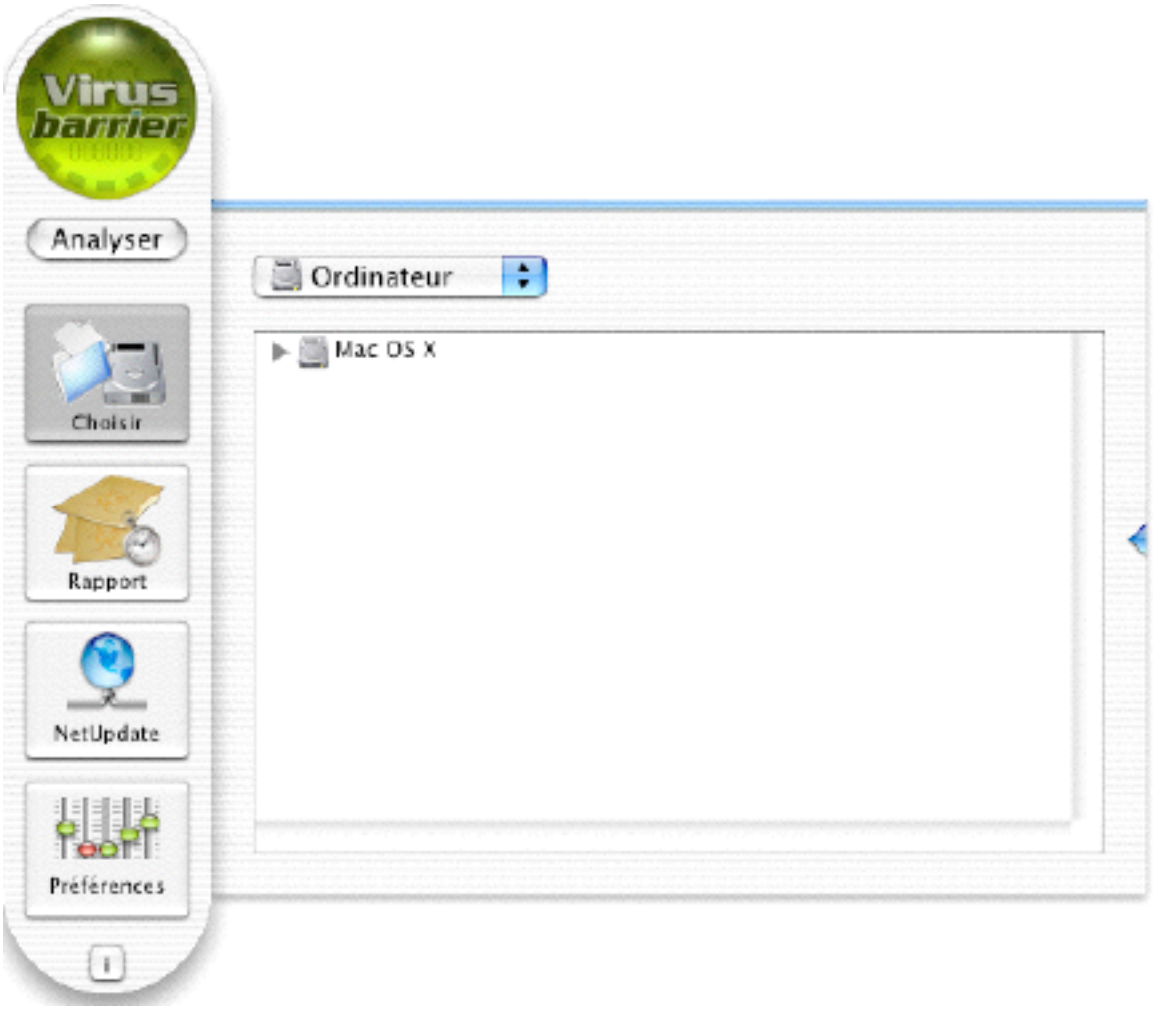
Analyse de virus

Intego VirusBarrier X fonctionne de plusieurs façons. Il surveille constamment votre ordinateur, vous protégeant des virus, et il vérifie automatiquement tous les supports amovibles, dès leur insertion dans le lecteur, qu'il s'agisse de CD-Rom, cartouches Zip ou autres. Il fonctionne également en mode manuel, ce qui vous permet d'analyser tout ordinateur, disque ou volume présent sur l'ordinateur ou un réseau.

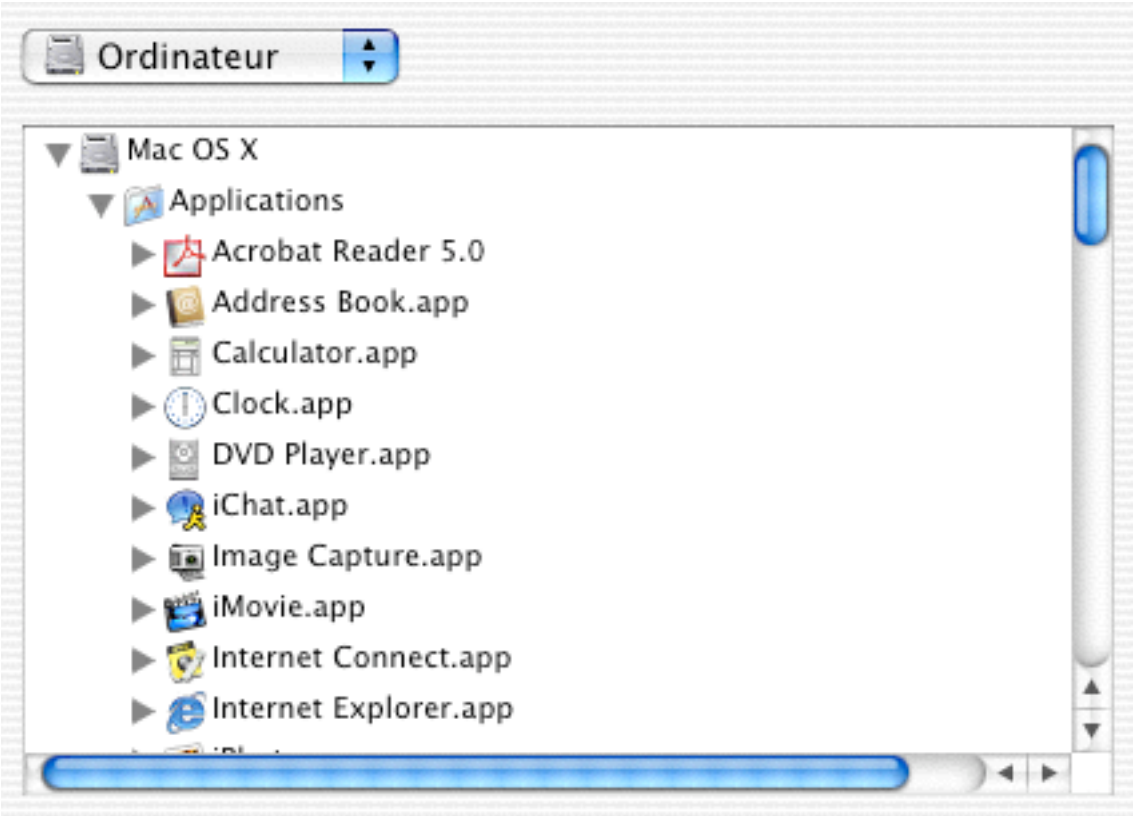
Analyse manuelle

Dès la première utilisation d'Intego VirusBarrier X, nous vous conseillons de procéder à une analyse complète de tous les disques durs ou volumes de votre ordinateur. Vous serez ainsi assuré de l'absence de virus cachés dans votre ordinateur. Cela peut être réalisé automatiquement dès l'installation du programme. Pour en savoir plus sur cette opération, reportez-vous au chapitre 3, Installation.

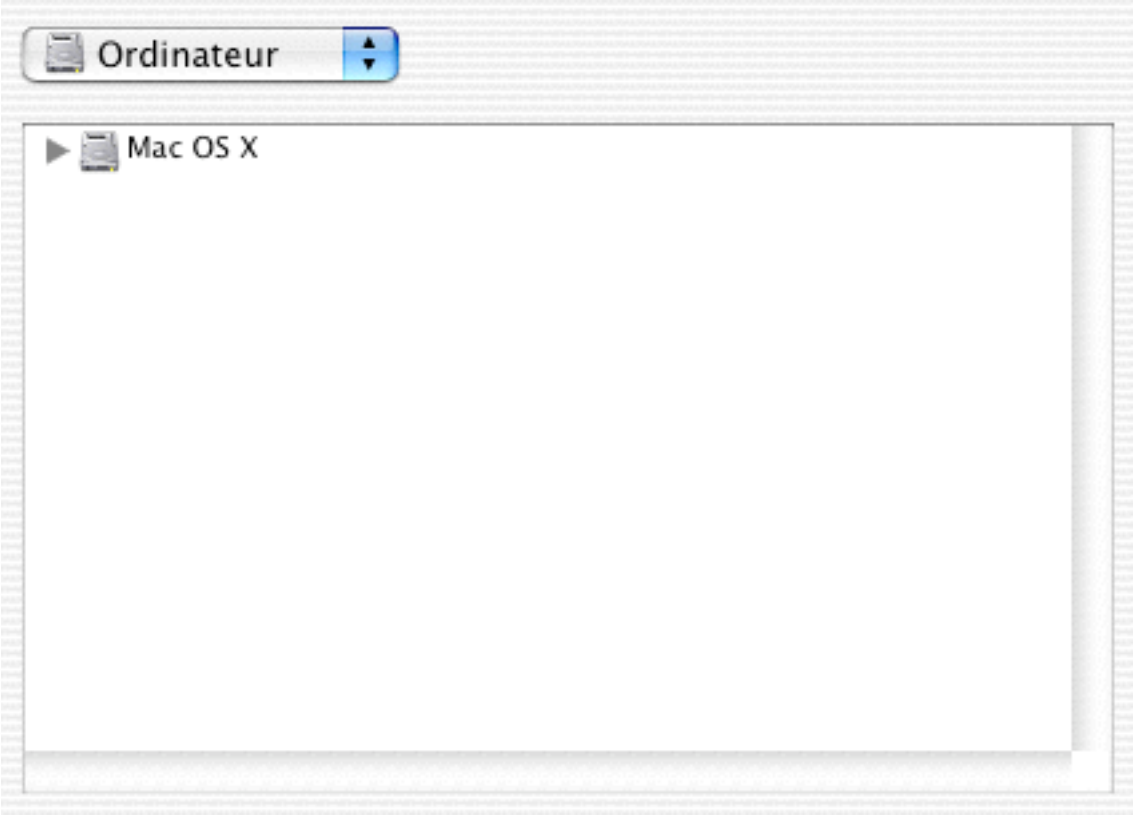
Vous pouvez également procéder à tout moment à une analyse manuelle sur tout volume, dossier ou fichier. Pour cela, ouvrez Intego VirusBarrier X et cliquez sur le bouton Choisir.



Un tiroir s'ouvre alors et présente tous les volumes montés sur votre ordinateur. Cette vue est de type liste du Finder, avec les volumes, les dossiers et les fichiers étant classés selon leur hiérarchie. Pour ouvrir un volume ou un dossier et en visualiser le contenu, cliquez sur le triangle à sa gauche ; tous les fichiers et dossiers seront listés au-dessous. Pour fermer un volume ou un dossier ouvert, cliquez sur ce même triangle.


Ordinateur
Mac OS X
Applications
Acrobat Reader 5.0
Address Book.app
Calculator.app
Clock.app
DVD Player.app
iChat.app
Image Capture.app
iMovie.app
Internet Connect.app
Internet Explorer.app

Analyser un volume



Pour analyser un volume, il suffit de double-cliquer dessus, ou bien cliquez une fois pour le sélectionner, puis cliquez sur le bouton Analyser. Vous constaterez le début de l'analyse d'après l'activité dans l'Orbe. Il indique d'abord le nombre de fichiers analysés en cours.

Si vous avez choisi Fichiers restant à analyser dans les Préférences, Intego VirusBarrier X compte le nombre de fichiers à analyser, puis affiche le nombre de fichiers restant à analyser et le pourcentage d'analyse restante. Si vous cliquez sur

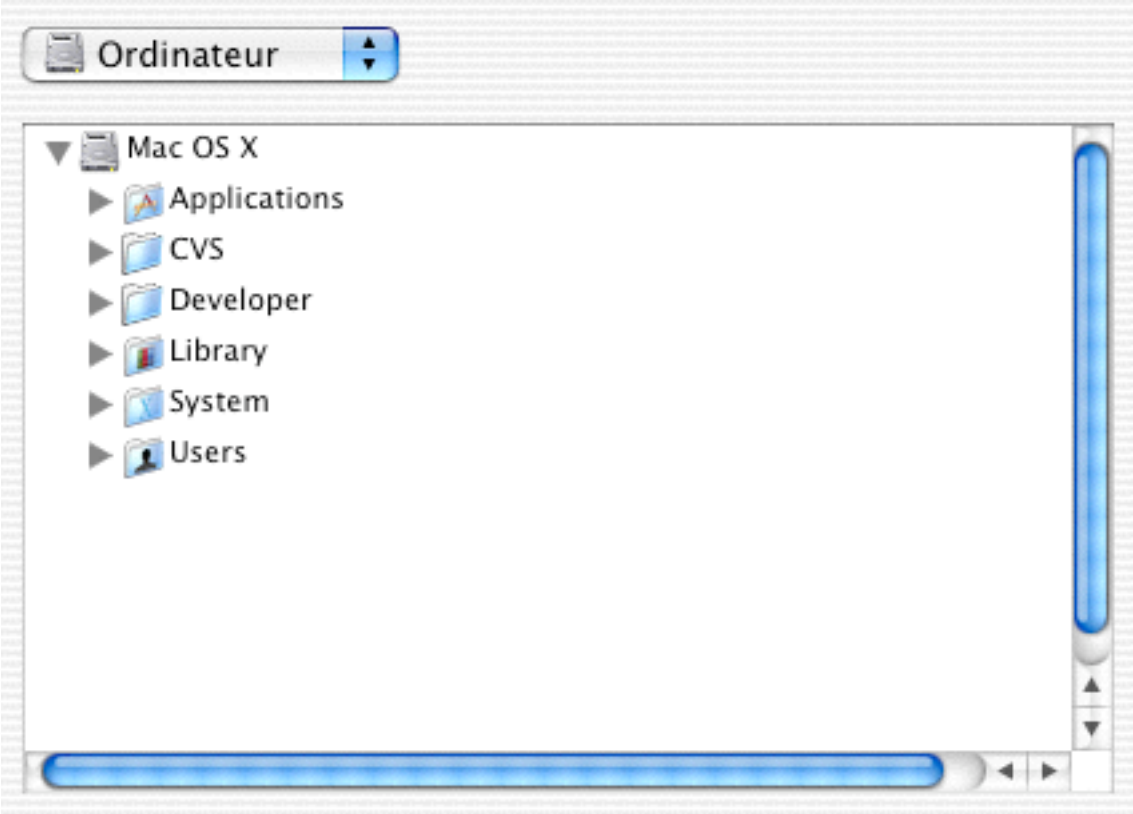
l'Orbe, l'affichage est modifié et indique le nombre de fichiers analysés et le pourcentage correspondant.

Vous pouvez arrêter l'analyse à tout moment en appuyant sur le bouton Stop.

Pour suspendre l'analyse, maintenez enfoncée la touche Maj de votre clavier, vous constaterez que le bouton Stop affiche alors Pause. Cliquez sur ce bouton et l'analyse marque un temps de pause.

Pour reprendre l'analyse, cliquez sur ce bouton, qui affiche alors Continuer.

Analyser un dossier



Pour analyser un dossier sur votre ordinateur, cliquez sur le triangle à gauche d'un volume et parcourez-le jusqu'à ce que vous ayez trouvé le dossier à analyser. Double-cliquez sur ce dossier, ou cliquez une fois pour le sélectionner, puis cliquez sur le bouton Analyser. Vous constaterez le début de l'analyse d'après l'activité dans l'Orbe. Il indique d'abord le nombre de fichiers analysés en cours.

Si vous avez choisi Fichiers restant à analyser dans les Préférences, Intego VirusBarrier X compte le nombre de fichiers à analyser, puis affiche le nombre de fichiers restant à analyser et le pourcentage d'analyse restante. Si vous cliquez sur

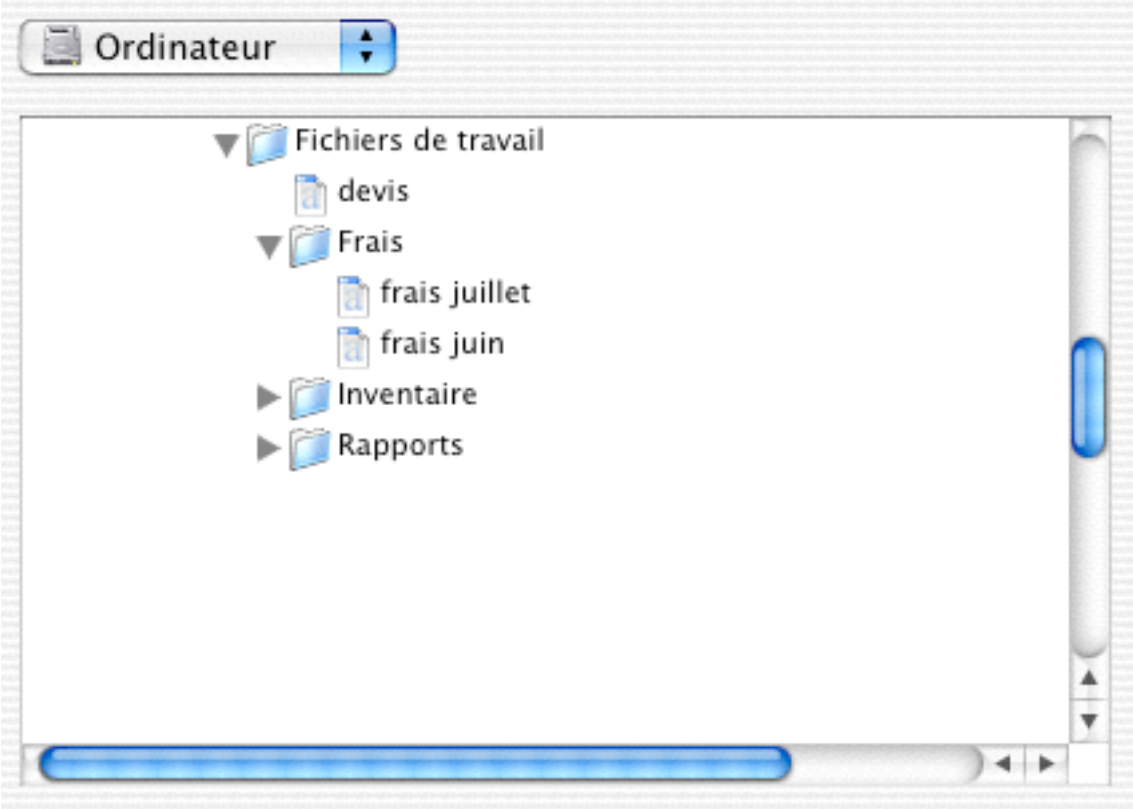
l'Orbe, l'affichage est modifié et indique le nombre de fichiers analysés et le pourcentage correspondant.

Vous pouvez arrêter l'analyse à tout moment en appuyant sur le bouton Stop.

Pour suspendre l'analyse, maintenez enfoncée la touche Maj de votre clavier, vous constaterez que le bouton Stop affiche alors Pause. Cliquez sur ce bouton et l'analyse marque un temps de pause.

Pour reprendre l'analyse, cliquez sur ce bouton, qui affiche alors Continuer.

Analyser un fichier



Pour analyser un fichier sur votre ordinateur, cliquez sur le triangle à gauche d'un volume ou d'un dossier et parcourez-le jusqu'à ce que vous ayez trouvé le fichier à analyser. Double-cliquez sur ce fichier ou cliquez une fois pour le sélectionner, puis cliquez sur le bouton Analyser. Vous constaterez le début de l'analyse d'après l'activité dans l'Orbe. Dans la plupart des cas, l'analyse d'un seul fichier est quasi immédiate.

Analyse en glisser-déposer

Vous pouvez également analyser un volume, un dossier ou un fichier en le faisant glisser sur n'importe quelle partie de l'interface d'Intego VirusBarrier X. Dès que vous le relâchez, Intego VirusBarrier X commence à l'analyser, comme c'est le cas pour toute analyse manuelle.

Résultat d'analyse

Si Intego VirusBarrier X trouve des fichiers infectés, la fenêtre du Rapport s'ouvre et présente les noms des fichiers, ainsi que le type de virus constaté. Si Intego VirusBarrier X est réglé pour la seule analyse, et non pas la réparation, il se contente de lister les fichiers concernés et le type de virus. Si le réglage d'Intego VirusBarrier X inclut la réparation automatique, vous disposerez des noms des fichiers réparés, ainsi que du type de virus.

Comprendre le résultat d'analyse

Intego VirusBarrier X vous informe de la détection de fichiers infectés par des virus connus. Il vous alerte également en cas de fichiers corrompus.

Fichiers infectés

En cas de détection de fichiers infectés, l'Orbe d'Intego VirusBarrier X devient rouge et le tiroir du Rapport s'ouvre, et cela dès la première détection ; il se peut que l'analyse soit toujours en cours au moment où le tiroir s'ouvre. Le mode d'alerte dépend également des options définies dans les Préférences. Pour en savoir plus sur les options d'alerte, reportez-vous au chapitre 6, Réglages d'Intego VirusBarrier X.

L'affichage dans le tiroir du Rapport dépend du mode d'analyse sélectionné dans les Préférences. En cas de détection de fichiers infectés ou corrompus, Intego VirusBarrier X peut procéder à des réparations automatiques (mode Réparation automatique), ou simplement vous alerter (mode Analyse). Le mode Réparation automatique entraîne des réparations immédiates, si c'est possible. Avec le mode

Analyse, les réparations doivent être faites manuellement. Pour en savoir plus sur ces deux modes, reportez-vous au chapitre 6, Réglages d'Intego VirusBarrier X.

Si vous avez choisi le mode Analyse, le tiroir du Rapport affiche le nom des fichiers infectés. Pour réparer ces fichiers, sélectionnez les éléments concernés et cliquez sur le bouton Réparer au bas de la fenêtre. La réparation sera faite et le tiroir du Rapport affichera ce changement. Pour visualiser les fichiers du Rapport dans le Finder et y accéder rapidement, cliquez sur un fichier pour le sélectionner et cliquez sur Afficher dans le Finder.

Analyser
Choisir
Rapport
NetUpdate
Préférences
Dernière analyse le Friday, September 6, 2002, 21:07
Infecté: 0
Réparé: 1
Corrompu: 0
Fichier: devis.doc était infecté par 'WM.Marker.A'.
Afficher dans le Finder
Réparer

Fichiers corrompus

En cas de détection de fichiers corrompus, le tiroir du Rapport d'Intego VirusBarrier X s'ouvre, et cela dès la première détection ; il se peut donc que l'analyse soit toujours en cours au moment où le tiroir s'ouvre. Le mode d'alerte dépend également des options définies dans les Préférences Pour en savoir plus sur les options d'alerte, reportez-vous au chapitre 6, Réglages d'Intego VirusBarrier X.

Les fichiers corrompus peuvent ne pas contenir de virus, mais beaucoup de virus risquent de corrompre les fichiers, sans même s'y copier. Les dommages peuvent provenir d'erreurs de disques ou de blocages alors que les fichiers sont ouverts. En cas de détection de fichiers corrompus, nous vous conseillons de les remplacer au plus tôt.

Alertes

Bien qu'Intego VirusBarrier X puisse réaliser des analyses manuelles, comme nous venons de le voir, il travaille habituellement en tâche de fond. Il dispose de diverses alertes en cas de détection de fichiers infectés.

Dans ce cas, si vous avez réglé Intego VirusBarrier X pour l'analyse, et non pas la réparation automatique des fichiers infectés, une alerte apparaît.

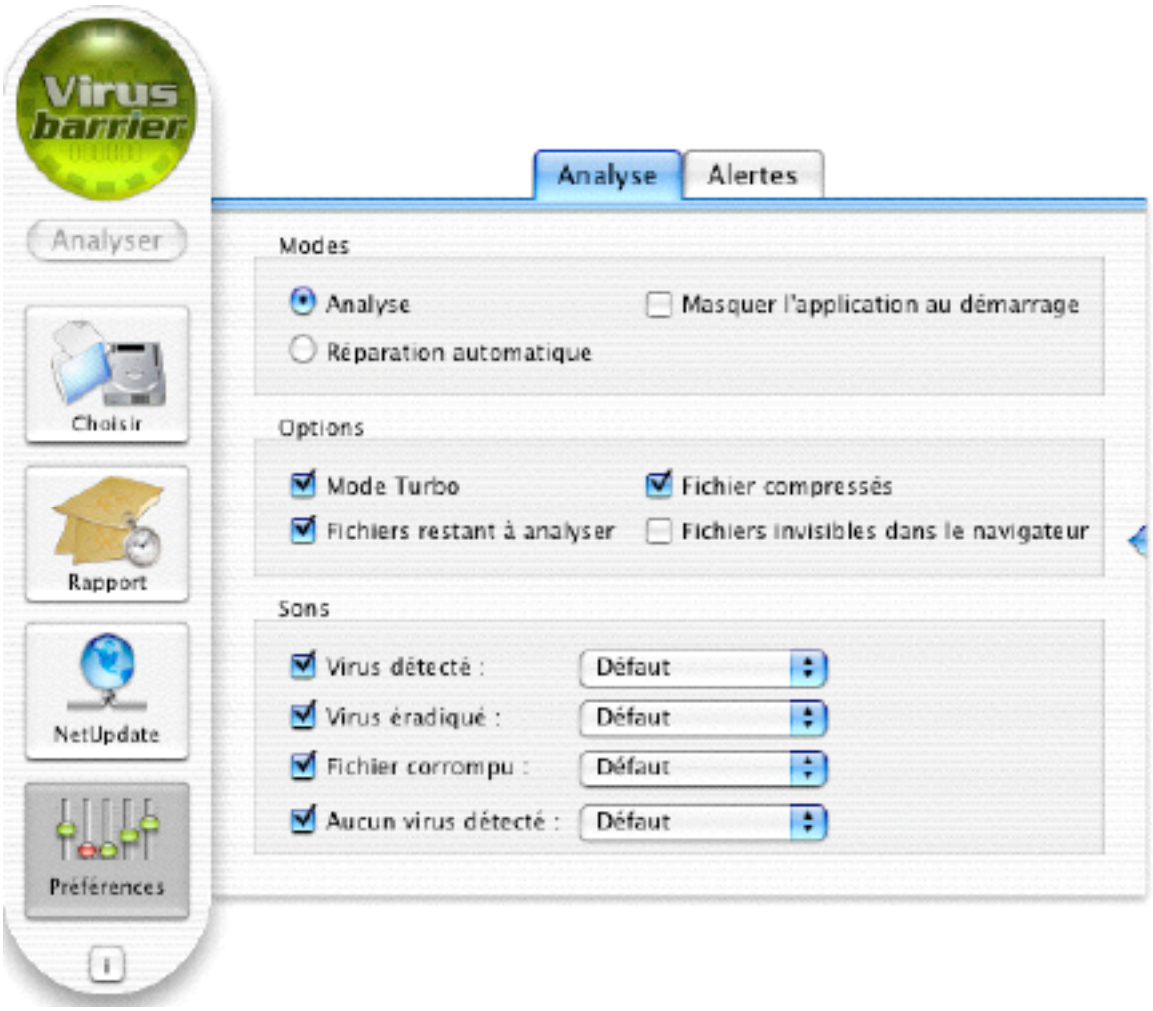
Si vous souhaitez qu'Intego VirusBarrier X répare le fichier, cliquez sur Réparer. Sinon, cliquez sur Ignorer cette alerte et le fichier ne sera pas réparé. Attention : cela peut être dangereux ! Choisissez de ne pas réparer ces fichiers uniquement si vous êtes sûr de ce que vous faites !

Pour en savoir plus sur les préférences d'alertes, reportez-vous au chapitre 6, Réglages d'Intego VirusBarrier X.

6 – Réglages d'Intego VirusBarrier X

Préférences

En cliquant sur le bouton Préférences de l'interface d'Intego VirusBarrier X, le tiroir présente deux onglets d'options : Analyse et Alertes.

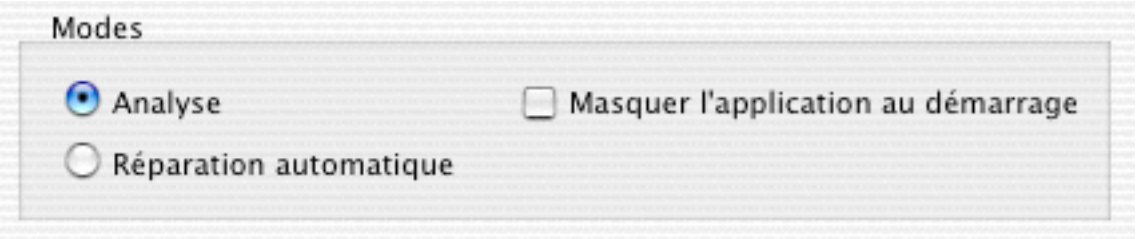


Analyse

Cet onglet permet le réglage des modalités d'analyse lors de la recherche de virus, et d'options concernant les informations fournies dans l'Orbe.

Modes

Cette partie traite le mode d'analyse et la visibilité de l'application au démarrage.



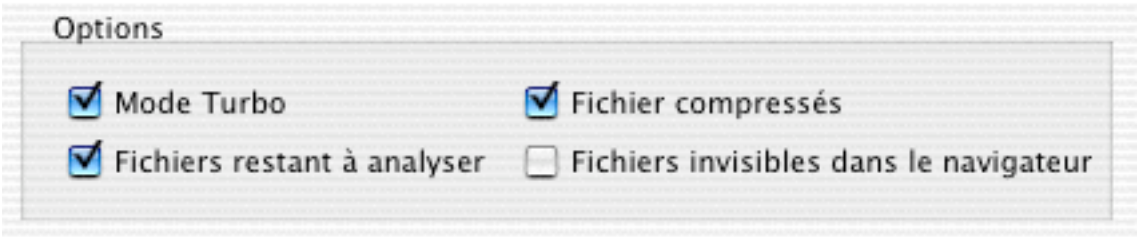
Intego VirusBarrier X dispose de deux modes d'examen des virus : Analyse et Réparation automatique. Si vous sélectionnez le mode Analyse, Intego VirusBarrier X vous alerte à chaque détection de fichiers infectés, mais il ne les répare pas automatiquement en les désinfectant. En cas de détection d'un fichier infecté, Intego VirusBarrier X vous alertera, ou, si vous exécutez une analyse manuelle, le Rapport affichera le fichier infecté, puis vous devrez réparer le fichier manuellement. Cela peut être utile si vous êtes sur un réseau et que votre administrateur de réseau a besoin d'examiner tout fichier infecté et détecté.

Pour sélectionner le mode d'analyse souhaité, cliquez sur le bouton radio correspondant.

Si vous sélectionnez Masquer l'application au démarrage, Intego VirusBarrier X apparaît dans le Dock au démarrage de l'application, mais l'application elle-même n'est pas visible. Vous pouvez analyser les fichiers, dossiers ou volumes en les faisant glisser sur l'icône Intego VirusBarrier X dans le Dock. Si Intego VirusBarrier X découvre des virus pendant ces analyses, vous recevez une alerte, selon les modalités choisies dans l'onglet Alertes.

Options

D'autres options contrôlent le fonctionnement d'Intego VirusBarrier X.



Mode Turbo

Si vous cochez la case Mode Turbo, Intego VirusBarrier X analyse les fichiers plus rapidement. A la première analyse de l'ordinateur, Intego VirusBarrier X se souvient de tous les fichiers examinés. Tant que ces fichiers ne sont pas mis à jour, Intego VirusBarrier X ne les réanalyse pas, ce qui rend l'analyse de 5 à 40 fois plus rapide. Cependant, dès qu'un fichier est modifié, il est analysé. De plus, après la mise à jour d'Intego VirusBarrier X intégrant de nouvelles définitions de virus, tous vos fichiers sont analysés pour s'assurer de l'absence de tous virus connus.

Fichiers restant à analyser

Si vous cochez cette option, pendant l'analyse, l'Orbe d'Intego VirusBarrier X affiche le nombre de fichiers restant à analyser plutôt que le nombre de fichiers déjà analysés.

Fichiers compressés

Si vous cochez Fichiers compressés, Intego VirusBarrier X analyse les fichiers compressés présents dans les archives Stuffit. Lors de l'analyse des fichiers compressés dans les archives Stuffit, une boîte de dialogue apparaît rapidement, et tous les fichiers infectés ou corrompus présents dans une archive sont signalés. Pour réparer ou désinfecter ces fichiers, vous devez décompresser l'archive, réparer ou désinfecter ces fichiers en les faisant glisser (fichiers ou dossiers) sur l'Orbe d'Intego VirusBarrier X, ou en les sélectionnant grâce au menu contextuel d'Intego VirusBarrier X. Ensuite, vous devez effacer l'archive originelle qui était infectée ou corrompue.

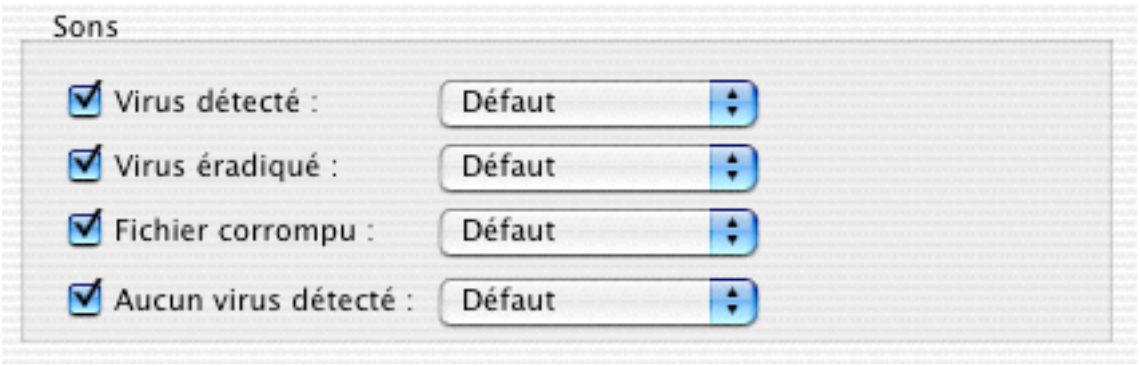
Fichiers invisibles dans le navigateur

Si vous cochez cette option, Intego VirusBarrier X affiche les fichiers invisibles dans le tiroir du navigateur.

Sons

Intego VirusBarrier X peut émettre un message vocal à la notification de quatre événements :

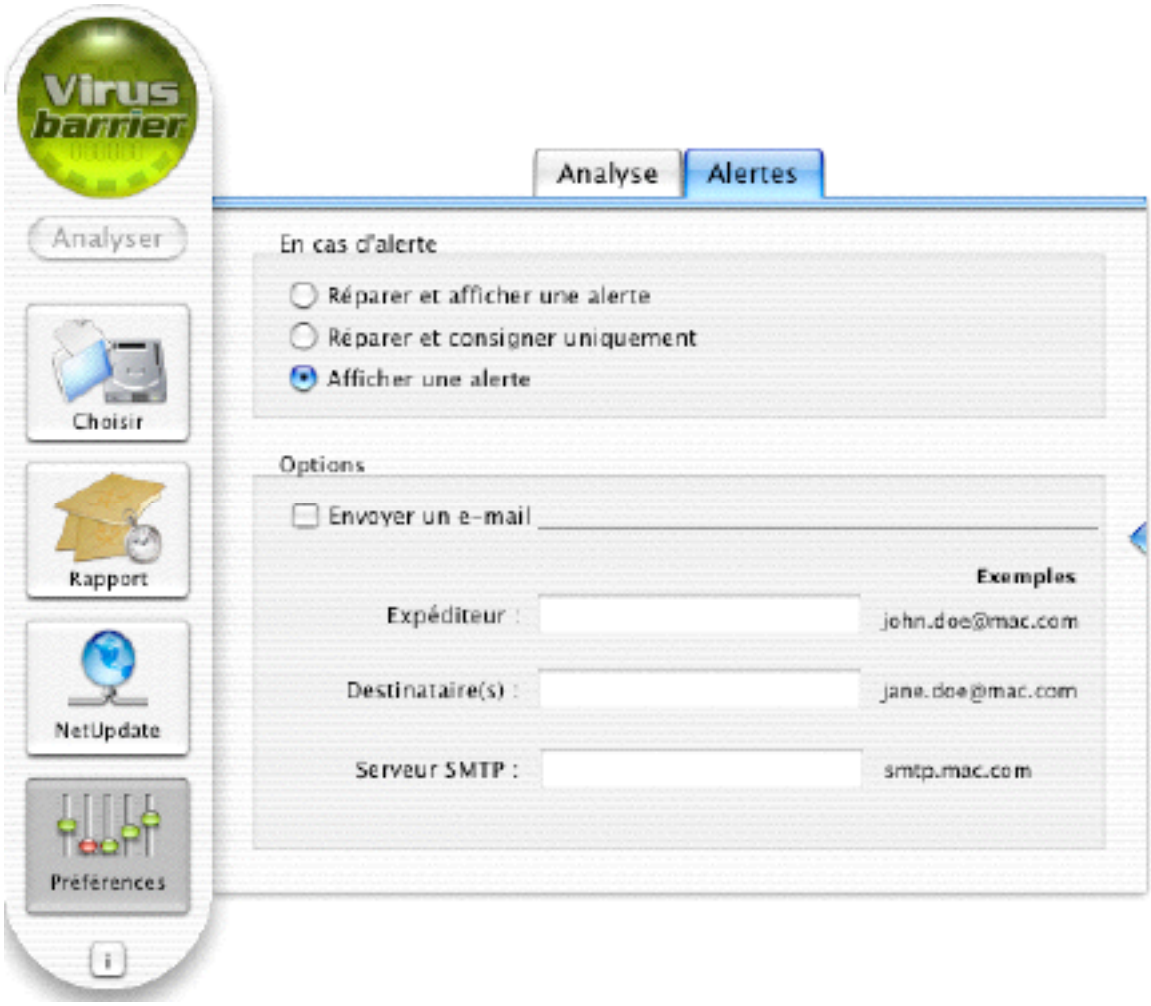
- Virus détecté
- Virus éradiqué
- Fichier corrompu
- Aucun virus détecté



Choisissez parmi les sons proposés par défaut, qui utilisent des voix synthétisées, ou sélectionnez tout autre son disponible sur l'ordinateur via le menu déroulant.

Alertes

Ce tiroir propose plusieurs modalités de réaction d'Intego VirusBarrier X en cas d'alerte.



Options d'alertes

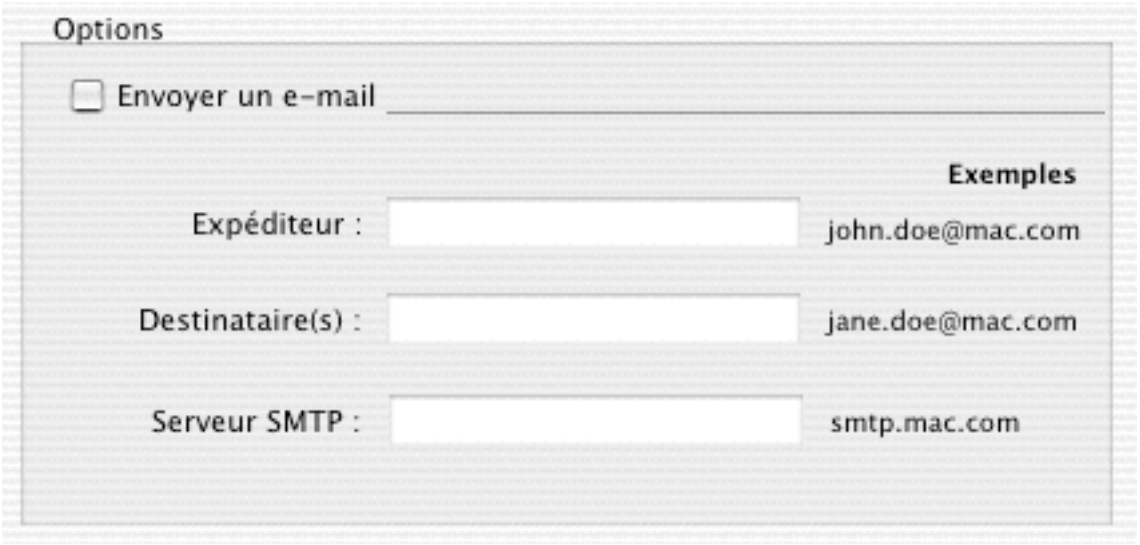
Trois options d'alerte sont possibles au cas où Intego VirusBarrier X détecte des virus dans les fichiers tout en travaillant en tâche de fond.

Réparer et afficher une alerte
Si cette option est cochée, Intego VirusBarrier X répare automatiquement les fichiers infectés et affiche une alerte vous informant du nom du fichier infecté et du virus trouvé.

Réparer et consigner uniquement
Si cette option est cochée, Intego VirusBarrier X répare automatiquement les fichiers infectés et enregistre le nom du fichier infecté et du virus trouvé dans son rapport. Il ne vous alerte pas, et vous devez vérifier le rapport pour connaître l'existence de fichiers infectés.

Afficher une alerte
Si cette option est cochée, Intego VirusBarrier X affiche une alerte vous informant du nom du fichier infecté et du virus trouvé. L'alerte demande si vous souhaitez réparer le fichier infecté.

Options



Envoyer un e-mail

Si cette option est cochée, Intego VirusBarrier X envoie automatiquement un message électronique aux destinataires indiqués, dans les 30 secondes. Vous devez entrer les adresses de l'expéditeur, du (ou des) destinataires et le serveur SMTP. Pour choisir plusieurs destinataires, entrez plusieurs adresses e-mail séparées par des virgules.

NetUpdate

Si vous cliquez sur le bouton NetUpdate, le tiroir correspondant s'ouvre. Ce tiroir permet la vérification des mises à jour, donne des informations sur la date de la dernière interrogation, le numéro de version d'Intego VirusBarrier X, et la date d'échéance de votre abonnement. Vous avez accès aux mises à jour du programme et des définitions de virus pendant un an à compter de la date d'achat d'Intego VirusBarrier X.

Pour rechercher les mises à jour, cliquez sur le bouton Interroger maintenant…. Intego NetUpdate s'ouvre et se connecte au serveur d'Intego à la recherche des mises à jour du programme ou des définitions de virus. Vous avez accès aux mises à jour du programme et des définitions de virus pendant un an à compter de la date d'achat d'Intego VirusBarrier X.

Vous pouvez régler NetUpdate, pour le choix des date et heure des mises à jour automatiques, dans le Panneau des Préférences NetUpdate sous les Préférences Système.

Pour en savoir plus sur NetUpdate et ses réglages, consultez le manuel NetUpdate.

Encyclopédie de virus

Le deuxième onglet de ce tiroir, Définitions de Virus, contient une encyclopédie des virus, proposant l'histoire de plusieurs virus Macintosh dont Intego VirusBarrier X vous protège.

A propos d'Intego VirusBarrier X

Ce tiroir donne des informations pratiques concernant Intego VirusBarrier X, telles que le numéro de version, votre numéro de support (dont vous avez besoin pour le support technique), des liens actifs au site Web et à l'adresse électronique d'Intego, ainsi que les coordonnées d'Intego.

Si vous souhaitez contacter Intego, cliquez sur le lien **Contact**. Votre programme de messagerie crée alors un nouveau message adressé à Intego, portant le sujet « Demande d'info du client » suivi de votre numéro de client. Tapez ensuite le texte de votre message et envoyez-le immédiatement à Intego.

Si vous avez besoin de contacter le support technique d'Intego, cliquez sur le lien **N° Support**. Votre programme de messagerie crée alors un nouveau message adressé à Intego, portant le sujet « Demande de support du client » suivi de votre numéro de client. Tapez ensuite le texte de votre message et envoyez-le immédiatement à Intego.

En cliquant sur le lien **Enregistrement**, vous allez à la page d'enregistrement d'Intego VirusBarrier X sur le site Web d'Intego. Il est important d'enregistrer votre programme pour pouvoir recevoir les dernières informations concernant Intego VirusBarrier X, Intego et ses autres produits.

En cliquant sur le lien Site Web, vous allez sur le site Web d'Intego.

7 - Diagnostic

Quelques symptômes d'infections

Bien que ces symptômes ne signifient pas nécessairement que votre ordinateur ait subi l'attaque d'un virus, ils peuvent en être le signe :

- messages d'erreur inattendus,
- votre Macintosh se bloque de façon inexplicable,
- les disques durs ou disquettes sont lus sans aucune raison apparente,
- le système est plus lent que d'habitude,
- l'espace disque semble avoir diminué de manière significative alors que vous n'avez pas fait l'ajout d'un grand nombre de fichiers.

Si votre ordinateur commence à présenter l'un de ces symptômes, il existe plusieurs moyens de vérifier si le problème vient d'un virus ou de questions logicielles.

Commencez par exécuter le programme Utilitaire de Disque d'Apple. Ce programme a été conçu pour diagnostiquer les problèmes de disque dur de votre ordinateur et en résoudre la plupart. Il est installé par défaut dans le dossier Utilitaires du dossier Applications. Si le programme Utilitaire de Disque identifie des problèmes qu'il ne peut résoudre, vous devrez vous procurer un logiciel commercial de maintenance de disque.

Si le problème persiste, il se peut qu'un logiciel récemment installé soit à l'origine du problème. En effet, la plupart des problèmes informatiques sont dus à des conflits de logiciels. Si vous venez d'installer de nouveaux logiciels, essayez de les désinstaller et vérifiez si le problème persiste.

Votre problème peut être causé par un périphérique, tel qu'un lecteur externe, un périphérique USB connecté à votre ordinateur, le pilote de votre imprimante, etc. À nouveau, vérifiez si le problème persiste lorsque ces périphériques et leurs pilotes sont désactivés.

Pour de plus amples informations, consultez la section Support du site Web Apple (www.apple.fr). Vous y trouverez peut-être une solution.

En dernier recours, si vous pensez être en possession d'un fichier infecté, vous pouvez envoyer une copie de ce fichier au centre de recherche de virus d'Intego. Pour de plus amples informations, reportez-vous au chapitre 8, Support technique.

Mesures de précaution élémentaires

Même si Intego VirusBarrier X veille à présent sur votre Macintosh, vous devez vous habituer à respecter quelques principes de base pour assurer une protection permanente de vos fichiers.

- Sauvegardez régulièrement vos fichiers. Avec le logiciel Intego Personal Backup X, automatisez vos sauvegardes.
- Créez plusieurs copies de vos fichiers les plus importants.
- Quand vos supports amovibles « voyagent » dans un autre ordinateur ou si vous les confiez à d'autres utilisateurs, veillez à les protéger en écriture en faisant coulisser la languette de protection (si possible).
- Sauf nécessité absolue, ne désactivez pas Intego VirusBarrier X : vous n'avez pas besoin de le désactiver pour installer de nouvelles applications, même si la plupart des programmes d'installation le demandent.
- N'utilisez pas de logiciels piratés : non seulement vous enfreignez les lois, mais ces programmes sont souvent porteurs de virus en raison de leur large diffusion.
- De même, n'installez les programmes que si vous êtes certain de l'intégrité de leur emballage d'origine.
- Pensez à utiliser régulièrement NetUpdate pour vérifier que votre version d'Intego VirusBarrier X est à jour.
- Pour éviter toute incompatibilité, utilisez uniquement Intego VirusBarrier X pour la protection de votre ordinateur contre les virus.

8 - Support technique

Le support technique est accessible aux utilisateurs d'Intego VirusBarrier X qui sont enregistrés.

Par courrier électronique

support@intego.com

Sur le site Web d'Intego

www.intego.com

Pour envoyer des fichiers au centre de recherche de virus d'Intego, contactez sendvirus@intego.com.

9 - Annexe

Glossaire

Antivirus – un antivirus est un programme qui protège votre ordinateur contre les virus en analysant, désinfectant et réparant les fichiers infectés. Il recherche des séquences de code correspondant à la " signature " du virus à certains emplacements dans les fichiers et les applications.
Archive – une archive contient plusieurs fichiers compressés pour économiser de l'espace disque. Le standard de compression sur Macintosh est Stuffit.
Boot – booter un ordinateur signifie le démarrer.
Canular – un canular est une fausse alerte de virus. Les canulars peuvent être diffusés par courrier électronique. Il y est toujours question de transmission de virus sur simple lecture d'un message électronique.
Cheval de Troie – un cheval de Troie est un programme derrière lequel se cache un code parasite. Étant donné qu'il ne se reproduit pas, il ne s'agit pas réellement d'un virus. Toutefois, il peut contenir un virus qui se copiera dans d'autres fichiers au moment de l'exécution du cheval de Troie. À l'origine, le cheval de Troie était un cheval de bois gigantesque et creux que les Grecs édifièrent et donnèrent soi-disant en cadeau aux Troyens. Ils amenèrent le cheval à l'intérieur de leur forteresse et, plus tard dans la nuit, les guerriers grecs sortirent du cheval, ouvrirent les portes de la cité, et leurs troupes stationnées à l'extérieur la prirent d'assaut.
Code – les programmes informatiques sont écrits sous forme de code (ou langage de programmation). Étant des programmes informatiques, les virus sont également écrits sous forme de code.
Extension – comme les tableaux de bord, les extensions (aussi appelées inits) font partie intégrante du système d'exploitation du Macintosh. Elles ajoutent des fonctions au système de base ou sont utilisées comme pilotes pour certains périphériques. Il existe deux types d'extensions : celles qui se chargent en même

temps que le système au démarrage de l'ordinateur, et celles qui sont appelées lorsque le système en a besoin.

Fichier Desktop – les fichiers Desktop sont des fichiers invisibles capables d'identifier la parenté entre les icônes et les fichiers et applications. Chaque volume (ou disque) de votre ordinateur contient des fichiers Desktop qui, sous Mac OS 9, sont appelés Desktop DB et Desktop DF. Votre ordinateur lit automatiquement ces fichiers chaque fois que vous insérez un support amovible dans un lecteur. Certains virus d'ancienne génération s'attaquent aux fichiers Desktop.

Infection – on dit qu'un fichier est infecté lorsqu'un virus s'est copié dans ce fichier. Il peut s'agir d'une macro copiée dans un fichier de traitement de texte, ou d'un autre type de code copié dans une application.

INIT – init est un autre terme pour désigner une extension. Il vient du fait que ces fichiers sont initialisés lors du démarrage de l'ordinateur.

Macro – une macro est un petit programme utilisant les fonctions intégrées du langage macro d'une application. Nombreuses sont les applications qui offrent des fonctions macro afin de faciliter l'exécution des tâches répétitives. Hélas, les macros peuvent contenir des virus et les macro virus en circulation sont très nombreux, notamment ceux qui s'exécutent sous Microsoft Word ou Excel.

Macro Commande – une macro-commande est une commande de programmation qui peut être exécutée dans une macro. Elle exploite le langage macro propre à l'application utilisée.

Macro Virus – un macro virus est un virus exploitant le langage macro intégré d'une application. Les macro virus sont actuellement les virus les plus redoutables pour les utilisateurs de Macintosh, particulièrement ceux qui s'exécutent sous Microsoft Word ou Excel, puisqu'ils sont transmissibles entre ordinateurs Macintosh et ordinateurs Windows.

Partition – une partition (ou volume) est une division logique de disque dur. Il est possible d'en créer plusieurs sur un disque dur. Chacune fonctionne alors comme

un petit disque dur. Le système d'exploitation considère les partitions comme des volumes distincts.

Ressource – les fichiers Macintosh se composent de deux parties : une partie ressources et une partie données. La partie ressources peut contenir des éléments tels que des icônes, du code ou des instructions pour applications. Certains virus se cachent dans les ressources. Ils peuvent également les corrompre ou les modifier.

Support amovible – tout support de stockage de données s'insérant dans un lecteur, tel que CD-ROM, cartouche Zip ou disquette.

Souche – une souche est une variante ou une mutation de virus. De la même manière qu'il est employé en médecine pour désigner les mutations de virus biologiques, ce terme s'applique aux virus informatiques qui, dans certains cas, subissent une mutation et donnent naissance à de nouvelles souches.

Ver – un ver est un programme qui se propage sur un réseau en s'auto-reproduisant. Du fait de leur capacité à nuire, on considère souvent les vers comme une variété de virus. Ils ne fonctionnent cependant pas de la même manière. Les vers n'ont pas besoin de fichiers hôtes pour se reproduire.

Virus – un virus est un programme informatique (c.-à.-d. une séquence de code informatique) capable de se reproduire et de se propager. La plupart des virus sont malveillants et infectent les fichiers en s'attachant à eux. Ils se propagent ensuite à l'ouverture ou à l'exécution des fichiers hôtes.

Volume – un disque dur ou un support amovible. Il peut s'agir d'un disque dur entier, d'une partition de disque dur, d'un ordinateur de réseau distant ou d'une disquette. Sa spécificité est qu'il contient ses propres fichiers répertoires indiquant où sont stockés les fichiers.

Encyclopédie des virus

ANTI

Le virus ANTI a vu le jour en France, en 1989. La première souche découverte fut baptisée ANTI-A ; la deuxième souche, ANTI-B, fut découverte en 1990. Ce virus infectait les applications mais ne s'attaquait pas aux fichiers Système ou aux fichiers de données. Il n'est efficace que sous le Système 6.

Le virus ANTI, dont le nom est tiré de la chaîne de caractères « ANTI » rencontrée dans le virus, était un virus relativement dangereux dans le mesure où il corrompait les applications et provoquait leur blocage. Les applications corrompues par le virus ANTI sont irréparables et doivent être réinstallées. Il semble toutefois que ce type de corruption soit fortuit, car le virus tente uniquement de se reproduire et n'a pas d'autres effets.

Selon toute vraisemblance, la souche ANTI-B a été écrite avant la souche ANTI-A. En effet, ANTI-A intègre un code qui neutralise ANTI-B. Il y a par ailleurs peu de différences entre les deux souches.

Vers AUTOSTART

C'est en mai 1998 que le premier ver infectant un ordinateur Macintosh a été découvert. Il s'est rapidement propagé dans le Sud-Est asiatique avant de gagner le monde entier. Il existe plusieurs variantes de ce ver : AutoStart 9805-A, B, C, D, E et F.

Ce ver se déploie facilement sur les ordinateurs Macintosh à la lecture d'un CD-ROM infecté, si la fonction « Lecture Automatique » de QuickTime est activée. Il s'autocopie sur l'ordinateur hôte, créant, dans le dossier Extensions, des fichiers invisibles, appelés Desktop Print Spooler, Desktop Printer Spooler, ou DELDesktop Print Spooler.

Ce ver peut endommager gravement votre ordinateur en supprimant des fichiers et en détruisant des données. Les différentes souches prennent pour cible différents types de fichiers. Les fichiers corrompus sont écrasés par des données parasites et ne peuvent être réparés ou restaurés. Les ordinateurs infectés font preuve d'une activité disque importante et inhabituelle toutes les 3, 6, 10 ou 30 minutes et peuvent faire apparaître Desktop Print Spooler dans le menu Applications.

CDEF

Le virus CDEF a été découvert en 1990 à Ithaca, New York. L'auteur de ce virus, qui a également écrit le virus MDEF, fut arrêté peu de temps après sa découverte. Son nom vient du fait qu'il utilise une ressource CDEF rencontrée dans le fichier Desktop pour se reproduire. Les ressources CDEF sont normalement présentes dans certaines applications et dans le fichier Système. Autrement dit, la présence de cette ressource ne signifie pas qu'un fichier soit infecté. Toutefois, la présence de cette ressource dans des fichiers Desktop est anormale.

Ce virus n'infectait que les fichiers Desktop et pouvait se propager très facilement d'un disque à un autre, étant donné que le Macintosh lit les fichiers Desktop de chaque disque monté. Le virus ne provoquait aucun dommage intentionnel, mais, à l'instar de nombreux virus, il pouvait se montrer dangereux.

Une deuxième version du virus CDEF a été découverte en 1993, mais cette nouvelle souche différait peu de celle d'origine.

CODE 1

CODE 1 a été découvert aux États-Unis en 1993. Ce virus n'était pas extrêmement virulent et infectait le fichier Système et les applications. Il renommait le volume de démarrage « Trent Saburo » si l'ordinateur était démarré un 31 octobre. Bien qu'il fût transmissible à d'autres ordinateurs, les seuls dommages causés étaient des blocages du Système et de certaines applications.

CODE 252

Le virus CODE 252 a été découvert aux États-Unis en 1992. Il infectait le fichier Système et les applications et affichait le message suivant sur l'écran des ordinateurs infectés et démarrés entre le 6 juin et le 31 décembre :

> You have a virus.
> Ha Ha Ha Ha Ha Ha Ha
> Now erasing all disks...
> Ha Ha Ha Ha Ha Ha Ha
> P.S. Have a nice day
> Ha Ha Ha Ha Ha Ha Ha
> (Click to continue...)

Malgré ce message, aucun fichier n'était supprimé par le virus. Aux autres époques de l'année (c.-à.-d., avant le 6 juin), le virus se copiait uniquement dans le fichier Système à partir d'applications, avant de se propager à d'autres applications. Bien que des blocages et des altérations de fichiers aient été observés sous le Système 7,

le virus ne pouvait pas se propager à d'autres applications sous cette version-là du système. En revanche, ce virus mal écrit pouvait provoquer d'autres blocages et dommages du fait de plusieurs erreurs contenues dans le code.

CODE 9811

Le virus CODE 9811 a été découvert en novembre 1998 en Suède. Il cache les applications et les remplace par des fichiers parasites dont les noms se composent de lettres aléatoires. Les lundis, la probabilité que le virus affiche le message « You have been hacked by the Praetorians » (Vous avez été piraté par les prétoriens) et qu'il orne le bureau de l'ordinateur infecté de vers électriques est de 25 %. Le virus tente par ailleurs de supprimer les logiciels antivirus présents dans le volume de démarrage.

CODE 32767

Ce virus très rare, qui n'est peut-être plus en circulation, a été découvert en 1997. Une fois par mois, il tente de supprimer des documents.

Flag

Le virus Flag (également appelé virus WDEF-C) infecte le fichier Système et, bien que son intention ne soit pas d'engendrer des dommages majeurs, il écrase la ressource WDEF portant l'ID 0. Cette action peut provoquer des dégâts. Ce virus n'est peut-être plus en circulation.

Frankie

Le virus Frankie, d'origine allemande, est un virus rare qui ne s'attaque qu'à certains émulateurs Macintosh fonctionnant sur les ordinateurs Atari ou Amiga. Il semble prendre pour cible les logiciels d'émulation piratés. Il affiche le message « Frankie says: No more piracy! » (Frankie dit : plus de piratage !) et provoque le blocage de l'ordinateur Atari. Bien qu'il n'ait aucun effet sur les ordinateurs Macintosh, il infecte les applications, et les copies d'applications infectées peuvent entraîner la propagation de ce virus à d'autres copies de l'émulateur.

Graphics Accelerator

Voir SevenDust.

INIT-M

Le virus INIT-M a été découvert aux États-Unis en 1993. Très dangereux, ce virus a été programmé pour se manifester tous les vendredis 13. Il peut endommager un grand nombre de dossiers et de fichiers en les renommant à partir de chaînes de caractères aléatoires. Il transforme également les créateurs et les types de fichiers en chaînes de 4 caractères aléatoires, ce qui modifie les icônes des fichiers et les rend inutilisables, à moins que ces informations soient restaurées dans leur état d'origine. Il redéfinit les dates de création et de modification des fichiers au 1er janvier 1904. Dans certains cas, le virus supprime les fichiers et peut également provoquer un affichage erroné des fenêtres.

Ce virus peut infecter tous types de fichiers et crée par ailleurs un fichier appelé « FSV Prefs » dans le dossier Préférences.

INIT 17

INIT 17 a été découvert au Canada en 1993. Il infecte le fichier Système et les applications. Lorsque les ordinateurs infectés étaient démarrés après 6h06'06", le matin du 31 octobre 1993, ce virus affichait le message « From the depths of Cyberspace » (Des profondeurs du cyberespace). Ce message n'apparaissait qu'une seule fois.

Étant truffé d'erreurs, ce virus pouvait provoquer des blocages sur certains ordinateurs Macintosh avec des processeurs 68000. Ces dommages étaient plus accidentels qu'intentionnels.

INIT 29

La première découverte de ce virus remonte à 1988, et une deuxième souche a été identifiée en 1994. Elles sont parfois appelées INIT 29 A et INIT 29 B.

Ce virus extrêmement dangereux infecte les fichiers Système, les applications et les documents. Cependant, les documents infectés ne peuvent pas contaminer d'autres fichiers.

Bien que ce virus ne cause aucun dommage intentionnel, outre le fait qu'il essaie de se propager, il affiche le message suivant si vous insérez une disquette verrouillée dans votre ordinateur :

> The disk "xxxx" needs minor repairs. (Le disque «xxxx» a besoin de réparations mineures.)
> Do you want to repair it? (Souhaitez-vous le réparer ?)

De plus, divers types de problèmes ont été observés sur des ordinateurs infectés, tels que des blocages, diverses erreurs et autres problèmes d'impression.

INIT 1984

Le virus INIT 1984 a été découvert en 1992 aux Pays-Bas et aux États-Unis. Comme de nombreux autres virus, il se déclenche lorsqu'un ordinateur infecté est démarré un vendredi 13. Comme le virus INIT-M, il peut endommager un grand nombre de dossiers et de fichiers en les renommant à partir de chaînes de caractères aléatoires. Il transforme également les créateurs et les types de fichiers en chaînes de 4 caractères aléatoires, ce qui modifie les icônes des fichiers et les rend inutilisables, à moins que ces informations soient restaurées dans leur état d'origine. Il redéfinit les dates de création et de modification des fichiers au 1er janvier 1904.

Ce virus n'infecte que les INIT (ou extensions) et n'infecte pas d'autres types de fichier. Il ne se propage pas aussi rapidement que d'autres virus affectant les applications, car l'échange d'INIT entre ordinateurs est relativement rare.

INIT 9403

Ce virus, également appelé virus SysX, a été découvert en Italie en 1994. Jusqu'à présent, il n'a infecté que des Macintosh exécutant une version italienne du Système. Très virulent, ce virus supprime des fichiers et tente d'effacer les disques montés. Il semble que ce virus ait été propagé par le biais de logiciels piratés. Il infecte le Finder ainsi que certains programmes de compactage et d'archivage.

Macro virus

Les macro virus constituent actuellement la plus grande menace pour les utilisateurs de Macintosh. Le premier véritable macro virus découvert fut le virus Concept, qui s'attaquait aux fichiers Microsoft Word. D'autres variantes lui emboîtèrent rapidement le pas, les concepteurs de virus ayant compris que l'ubiquité de ce programme présentait un potentiel destructeur remarquable. Plus tard, des macro virus allaient être écrits pour exploiter également Microsoft Excel. En l'espace de 5 ans après l'apparition de ce premier virus, plusieurs milliers de macro virus allaient être découverts.

Le véritable danger des macro virus vient du fait qu'il s'agit des premiers virus multi-plates-formes. Pendant des années, les utilisateurs de Macintosh pouvaient s'estimer à l'abri des virus, sachant que seules quelques dizaines de virus menaçaient les ordinateurs Macintosh, contre plusieurs milliers pour Windows. Mais avec la forte dissémination des macro virus, le danger est plus présent.

La majorité des macro virus prennant pour cible les fichiers Microsoft Word utilisent des commandes telles que AutoOpen, AutoClose, AutoExec et AutoExit. Ces commandes s'exécutent lorsqu'un certain événement intervient dans le fichier, et ces quatre événements se produisent à chaque utilisation de fichier. Une macro, écrite pour se copier uniquement à l'exécution d'une certaine commande de menu, aura plus ou moins de chances de se propager.

De manière générale, les macro virus agissent à l'ouverture d'un fichier en se copiant dans le modèle qui s'est également ouvert. Ce modèle, vous ne l'avez pas ouvert à proprement parler. De fait, il est toujours ouvert en arrière-plan – il contient certaines informations de personnalisation, telles que des barres d'outils, ainsi que les macros légitimes éventuellement ajoutées.

Le macro virus type qui affecte Microsoft Word se copie dans le modèle actif, modifie certains éléments de menu de manière que vous ne puissiez pas modifier le modèle, change les types de fichier (leurs icônes sont modifiées, donnant ainsi l'impression qu'il s'agit de modèles), puis se copie à partir du modèle corrompu dans tous les nouveaux fichiers créés ou ouverts. Ce virus peut être supprimé s'il est détecté à temps. Il suffit de supprimer le fichier modèle actif et les fichiers infectés.

D'autres macro virus risquent d'être beaucoup plus dangereux. Ils peuvent endommager ou supprimer vos fichiers, masquer certaines fonctions d'applications, et plus encore. Et, pour couronner le tout, ce sont des virus multi-plates-formes qui endommagent aussi bien les ordinateurs Macintosh que les PC fonctionnant sous Windows.

MacMag

Le virus MacMag est un exemple de bonnes intentions qui ont tourné au vinaigre. Écrit pour le magazine MacMag, il avait été conçu pour afficher un message de paix lors du démarrage des ordinateurs infectés le 2 mars 1998, avant de s'autodétruire. À l'origine, il résidait dans une pile HyperCard appelée New Apple Products (qui, de fait, était un cheval de Troie), et se propageait en infectant le fichier Système. Il n'est probablement plus en circulation, mais certains disques et CD-ROM anciens peuvent encore l'abriter.

MBDF

Ce virus a été découvert au Pays de Galles en 1992 grâce à la fonction interne de détection de virus des applications Claris. À l'origine, il a été transmis par les jeux 10 Tile Puzzle et Obnoxious Tetris et par un cheval de Troie appelé Tetricycle.

Dans ce cas particulier, le virus MBDF a conduit à l'arrestation et à la condamnation de deux étudiants américains.

Le virus infecte les applications et le fichier Système en copiant une ressource MBDF portant l'ID 0. Si, cependant, le fichier Système comprend déjà une ressource avec ce nom, il n'est pas modifié.

Bien que non nuisible, ce virus peut endommager le Système. Il engendre par ailleurs certains problèmes liés aux menus. Les deux souches existantes, MBDF A et MBDF B, sont très similaires.

MDEF

Il existe quatre souches du virus MDEF : A, B, C et D. La souche A est parfois appelée virus Garfield, et la souche B est connue sous le nom de virus Top Cat. Elles ont été découvertes en 1990 et 1991 à Ithaca, New York. L'auteur de ce virus, également auteur du virus CDEF, fut arrêté peu de temps après cette découverte.

Le nom vient du fait qu'il utilise une ressource MDEF pour se reproduire. Les ressources MDEF sont normalement présentes dans certaines applications et dans le fichier Système. Autrement dit, la présence de cette ressource ne signifie pas qu'un fichier soit infecté.

Ce virus s'attaque aux applications ainsi qu'au fichier Système et peut également infecter les documents et les fichiers Desktop. Même si l'intention de son auteur n'était pas de provoquer des dommages, ce virus peut s'avérer nuisible. Il peut en effet endommager certaines applications et d'autres types de fichier.

MDEF 666

Voir SevenDust.

MDEF 9806

Voir SevenDust.

nVIR

Le virus nVIR a été découvert en Europe en 1987. Il existe deux souches principales : nVIR A et nVIR B. Ce virus est également connu sous d'autres noms, tels que AIDS, Fuck, Hpat, Jude, MEV# et nFlu.

Sans provoquer de dommages intentionnels, ce virus se reproduit en infectant le fichier Système et les applications. Il émet un bip ou engendre le message vocal « Don't panic » si MacinTalk est installé. La probabilité d'occurrence de ces événements au démarrage de l'ordinateur est variable.

Scores

Scores, également connu sous le nom d'Eric, Vult, NASA et San Jose Flu, a été identifié pour la première fois en 1998 aux États-Unis. Son auteur l'aurait écrit pour étudier le comportement des virus, mais il s'est propagé rapidement. Il crée deux fichiers invisibles appelés Scores et Desktop_, infecte le fichier Système et corrompt les fichiers Calepin et Album en modifiant leurs icônes. Il se propage ensuite aux autres applications que vous exécutez, mais sans les infecter toutes. Il peut

également provoquer des blocages intempestifs ainsi que des problèmes d'impression.

SevenDust

Il existe plusieurs souches du virus SevenDust, chacune étant désignée par une lettre comprise entre A et G. Il est également connu sous les noms MDEF 9806 et MDEF 666. Ces virus se propagent à travers les ressources MDEF, MENU ou WIND et une extension. SevenDust E, également connu sous le nom de Graphics Accelerator, a vu le jour dans un cheval de Troie en 1998.

Cette famille de virus peut infecter les applications, le fichier Système et les tableaux de bord. Ils tentent de supprimer tous les fichiers qui ne sont pas des applications dans le volume de démarrage lorsque l'ordinateur fonctionne entre 6 et 7 heures du matin, les 6 et 12 de chaque mois.

La souche SevenDust F s'est propagée par le biais d'un cheval de Troie appelé ExtensionConflict, et elle se subdivise en cinq souches inférieures qui se propagent via d'autres extensions.

SysX

Voir INIT 9403.

T4

Le virus T4 a été découvert en 1992. Il était intégré au jeu GoMoku, versions 2.0 et 2.1, autrefois disponible sur plusieurs sites FTP. Ce virus infecte les applications et

le Finder, et tente d'altérer le fichier Système. Il se fait également passer pour l'antivirus freeware Disinfectant afin de tromper les autres programmes antivirus.

Il peut provoquer des dommages irréparables sur le fichier Système ainsi que des blocages intempestifs. Il peut également empêcher l'amorçage de votre ordinateur.

Une autre souche, T4-D, a été découverte en 1997. Elle supprime des fichiers et des documents dans le dossier Système, mais pas le fichier Système lui-même. Elle se propage d'une application à une autre en s'attachant à la ressource CODE de l'application.

WDEF

Le virus WDEF, découvert en Belgique en 1989, tire son nom de la ressource WDEF présente dans le fichier Desktop. Ses deux souches, WDEF A et B, se propagent en infectant ces fichiers. Étant donné que le Système lit les fichiers Desktop de chaque disque monté, le virus peut se propager très facilement, sans même qu'il soit nécessaire d'exécuter des applications.

Bien qu'il ne provoque aucun dommage intentionnel, certaines de ses erreurs de programmation peuvent engendrer des problèmes, tels que des blocages et des problèmes d'affichage de polices.

ZUC

Le virus ZUC a été découvert en 1990. Il tire son nom de la personne qui l'a découvert : Don Ernesto Zucchini. Il existe trois variantes de ce virus : ZUC A, B et C. Elles n'infectent que les applications et peuvent se propager même si les

applications ne sont pas exécutées. Elles engendrent un comportement anormal du curseur mais n'ont aucun autre effet négatif.